Spectralink 84-Series Wireless Telephone

# AudioCodes Gateway and Avaya Communication Manager

## Interoperability Guide

1725-86914-000 Rev. C
September 2013

## Copyright Notice

© 2013 Spectralink Corporation All rights reserved. Spectralink™, the Spectralink logo and the names and marks associated with Spectralink's products are trademarks and/or service marks of Spectralink Corporation and are common law marks in the United States and various other countries. All other trademarks are property of their respective owners. No portion hereof may be reproduced or transmitted in any form or by any means, for any purpose other than the recipient's personal use, without the express written permission of Spectralink.

All rights reserved under the International and pan-American Copyright Conventions. No part of this manual, or the software described herein, may be reproduced or transmitted in any form or by any means, or translated into another language or format, in whole or in part, without the express written permission of Spectralink Corporation.

Do not remove (or allow any third party to remove) any product identification, copyright or other notices.

## Notice

Spectralink Corporation has prepared this document for use by Spectralink personnel and customers. The drawings and specifications contained herein are the property of Spectralink and shall be neither reproduced in whole or in part without the prior written approval of Spectralink, nor be implied to grant any license to make, use, or sell equipment manufactured in accordance herewith.

Spectralink reserves the right to make changes in specifications and other information contained in this document without prior notice, and the reader should in all cases consult Spectralink to determine whether any such changes have been made.

NO REPRESENTATION OR OTHER AFFIRMATION OF FACT CONTAINED IN THIS DOCUMENT INCLUDING BUT NOT LIMITED TO STATEMENTS REGARDING CAPACITY, RESPONSE-TIME PERFORMANCE, SUITABILITY FOR USE, OR PERFORMANCE OF PRODUCTS DESCRIBED HEREIN SHALL BE DEEMED TO BE A WARRANTY BY SPECTRALINK FOR ANY PURPOSE, OR GIVE RISE TO ANY LIABILITY OF SPECTRALINK WHATSOEVER.

## Warranty

The *Product Warranty and Software License and Warranty* and other support documents are available at http://support.spectralink.com.

## Contact Information

US Location
800-775-5330

Spectralink Corporation
2560 55th Street
Boulder, CO 80301

info@spectralink.com

Denmark Location
+45 7560 2850

Spectralink Europe ApS
Langmarksvej 34
8700 Horsens

infodk@spectralink.com

# Contents


## Introduction ..... 7

**Who Should Read this Guide?** ..... 7
**Product Support** ..... 8
**Spectralink References** ..... 8
*Specific Documents* ..... 9
**AudioCodes References** ..... 9
**Conventions Used In This Document** ..... 10
*Icons* ..... 10
*Typography* ..... 12

## Part I: The AudioCodes Solution ..... 13

### Chapter 1: Test Overview ..... 14

**Results Overview** ..... 14
*The Test Equipment* ..... 15
**Network Topology** ..... 15
*Why Q.SIG?* ..... 17
*A Word about Wi-Fi* ..... 17

### Chapter 2: What the Mediant Gateway Does ..... 19

**How Stand Alone Survivability Application Works** ..... 20
*SAS Emergency State* ..... 20
*User Authentication* ..... 20

### Chapter 3: Features and Capacity ..... 21

**System Capacity Requirements** ..... 21
**Capacity Analysis** ..... 21
**Features Tested and Validated** ..... 22
*Footnotes* ..... 24

### Chapter 4: Unpacking and Familiarizing Yourself with the Mediant Gateway ..... 26

**Package Contents** ..... 26
*Front-Panel Description* ..... 26
*T1/E1 Module* ..... 27
*CRMX Module* ..... 28

*Rear-Panel Description* ..... *29*

**Chapter 5: Preparing the Mediant Gateway for Initial Configuration 30**

**Insert the T1/E1 Module** ..... **30**
**Connect to Power Connect to Computer** ..... **31**

**Part II: Configuring the Components ..... 32**

**Chapter 6: Initial Configuration of the Mediant Gateway ..... 33**

**1. Connect Mediant Gateway to a single computer** ..... **33**
*The Home screen* ..... *34*
*The Toolbar and Navigation pane* ..... *34*
*The Burn button* ..... *34*
*Navigation Pane* ..... *34*
*The Search option* ..... *35*
*Device Actions* ..... *35*
**2. Feature Key/License Verification and Upgrade** ..... **35**
*Verify License keys feature* ..... *35*
*Add Software upgrade key (optional if key needs to be installed)* ..... *36*
**3. Disable DHCP Client and Server** ..... **37**
*Disable the Device's DHCP Server* ..... *37*
*Disable the DHCP Client* ..... *38*
*Set DHCP Lease Renewal* ..... *39*
**4. Set Mediant Gateway IP Address** ..... **40**
*Verify the settings* ..... *41*
**5. Set NTP settings** ..... **43**
**6. Set Syslog Parameters** ..... **44**
*Set CDR Reporting* ..... *45*
*Configure additional syslog trace settings* ..... *46*
**7. Enable SAS Application** ..... **47**
*Configure SAS* ..... *48*
**8. Configure Mediant Gateway Application SIP parameters** ..... **50**
**9. Configure Mediant Gateway Trunk Group** ..... **51**
**10. Configure Mediant Gateway Trunk Group Settings** ..... **53**
**11. Configure Tel to IP Routing** ..... **55**
**12. Configure IP to Trunk Routing** ..... **56**
*Avoiding a Routing Loop* ..... *57*
*Detecting a routing loop* ..... *58*
**13. Configure Default Coder Group** ..... **59**
**14. Enable Early Media** ..... **60**
**15. TDM configuration** ..... **61**
**16. B-Channel negotiation** ..... **62**

**17. Setting up the PRI** ..... **63**
*Q931 Layer Response Behavior* ..... *66*
**18. Changing the Password** ..... **68**

**Chapter 7: Installing the Mediant Gateway** ..... **69**

**Mount the Mediant Gateway** ..... **69**
*Desktop mounting* ..... *69*
*19-inch Rack Mounting* ..... *70*
**Cabling the Mediant 1000** ..... **72**
*Connecting to Ground* ..... *72*
*Connecting to the LAN* ..... *72*
*Connecting to E1/T1 Trunks* ..... *73*
*Connecting to Power* ..... *74*

**Chapter 8: Test Basic Functionality** ..... **75**

**Chapter 9: Configuration Requirements of the Avaya Communication Manager** ..... **76**

**1. Q.SIG** ..... **76**
**2. Add or Change the DS1 to Support Q.SIG** ..... **81**
**3. Add Signaling Group to Trunk Group** ..... **82**
**4. Add a Trunk Group** ..... **83**
**5. Change Signaling Group** ..... **89**
**6. Set up Dialing Parameters** ..... **90**
**7. Change the Automatic Alternate Routing Table** ..... **91**
**8. Add the Route Pattern** ..... **92**

**Chapter 10: Expanding your System** ..... **93**

**Adding a Second Trunk Group on the Same PBX** ..... **93**
*1. Add another DS1* ..... *94*
*2. Add Signaling Group* ..... *94*
*3. Add a Trunk Group* ..... *96*
*4. Change Signaling Group* ..... *101*
*5. Set up Dialing Parameters* ..... *102*
*6. Change the Automatic Alternate Routing Table* ..... *103*
*7. Add the Route Pattern* ..... *104*
*8. Set Caller ID* ..... *104*
**Adding a Second PRI to an Existing Trunk Group on the PBX** ..... **105**
*1. Add the DS1* ..... *107*
*2. Add Signaling Group* ..... *107*
*3. Add Channels* ..... *109*
*4. Configure the AudioCodes Mediant Gateway* ..... *111*

# Part III: Deployment, Testing and Troubleshooting 115

## Chapter 11: Testing Mediant Gateway to PBX Functionality ..... 116

## Chapter 12: Troubleshooting ..... 117

**Features** ..... **117**
*Transfer* ..... *117*
*Call Forward* ..... *117*
*Caller ID* ..... *118*
**Resetting the Mediant Gateway** ..... **119**
*Clearing the configuration* ..... *119*
*Using the serial adapter cable* ..... *120*

# Part IV: Appendices ..... 121

## Appendix A: Module Maintenance ..... 122

## Appendix B: Software Upgrade Procedure ..... 123

## Appendix C: Sample Files ..... 127

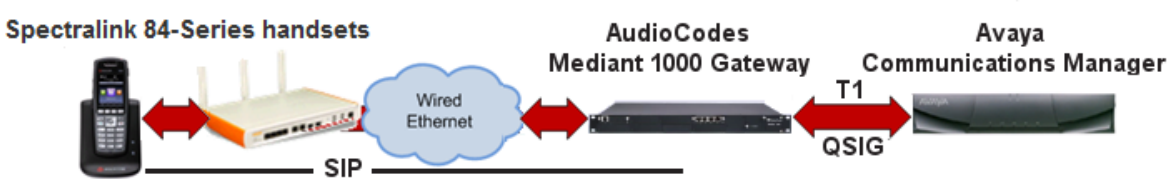
**Sample AudioCodes .ini file** ..... **127**
**Sample Phone Configuration Files** ..... **134**

## Appendix D: Information needed when you Contact Spectralink Support ..... 136

# Introduction

This guide will help you understand how the AudioCodes Mediant Gateway functions and offers configuration parameters for the Avaya PBX to establish interoperability.

This document describes a solution developed in Spectralink's wireless laboratories to deploy its advanced SIP wireless handsets, the 84-Series, within non-SIP telephony facilities. This solution is comprised of an Avaya Communication Manager and an AudioCodes MSBG Mediant Gateway which provides SIP service to Spectralink 84-Series SIP handsets.




The general test approach had the Spectralink 84-Series handsets register as SIP telephones with the AudioCodes gateway. The test verified that calls could be routed through the Avaya Communication Manager when PBX call routing was required, i.e. when connecting to a telephone other than the handsets registered to the same AudioCodes Mediant Gateway. The test also verified that the Spectralink handsets were able to call each other without going through the PBX. Basic telephony features were tested.

## *Who Should Read this Guide?*

This guide is designed for Spectralink system engineers who will be installing the AudioCodes devices and site-based system administrators and network engineers who may need to alter the LAN to accommodate the equipment. PBX administrators should be on hand to manage the PBX configuration requirements and test the system before its deployment.

# Product Support

Spectralink wants you to have a successful installation. If you have questions please contact the Customer Support Hotline at 1-800-775-5330.

The hotline is open Monday through Friday, 6 a.m. to 6 p.m. Mountain time.

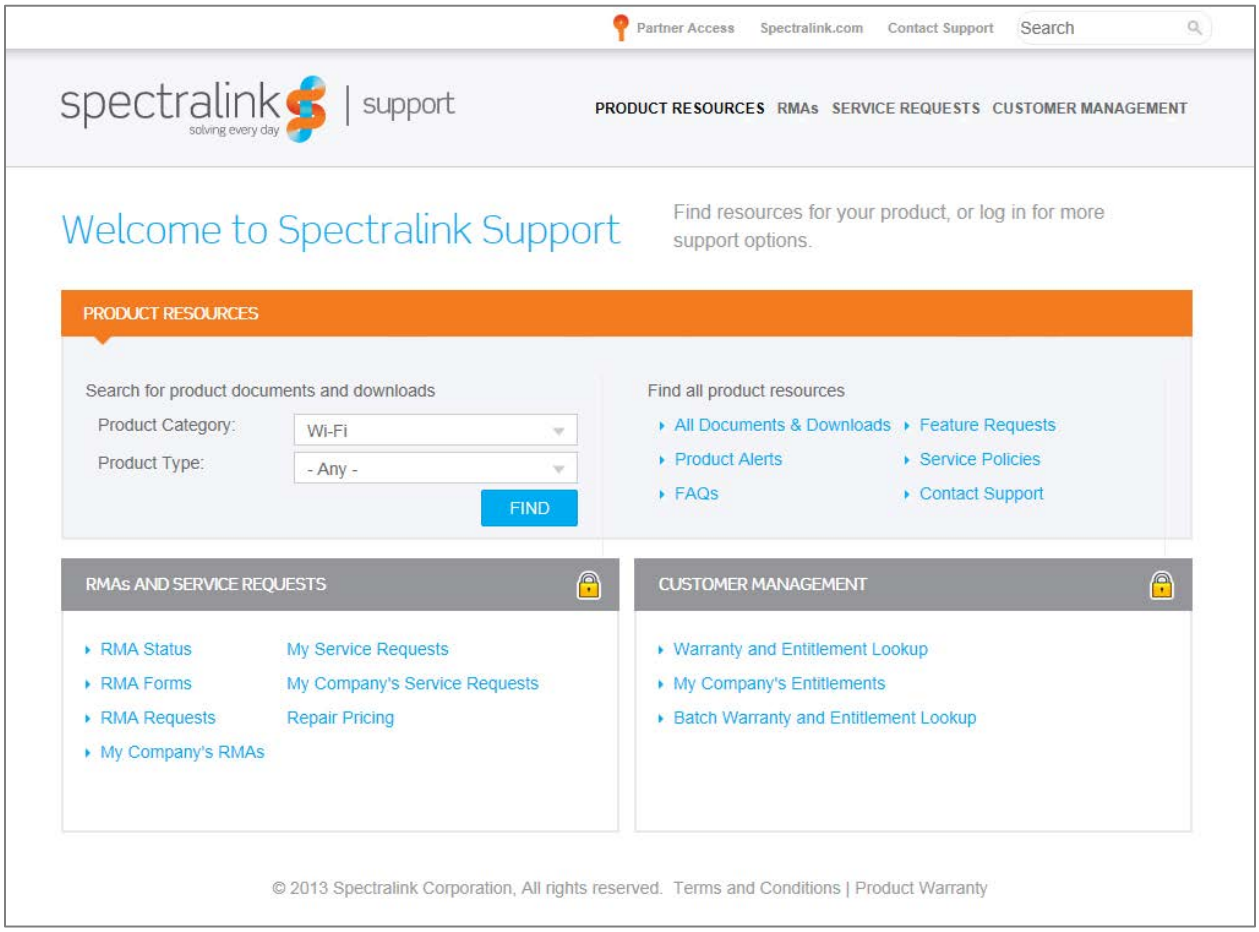
For Technical Support: mailto:technicalsupport@spectralink.com

For Knowledge Base: http://support.spectralink.com

For Return Material Authorization: mailto:nalarma@spectralink.com

# Spectralink References

All Spectralink documents are available at http://support.spectralink.com.




**To go to a specific product page:**

Select the Product Category and Product Type from the dropdown lists and then select the product from the next page. All resources for that particular product are displayed by default

under the All tab. Documents, downloads and other resources are sorted by the date they were created so the most recently created resource is at the top of the list. You can further sort the list by the tabs across the top of the list to find exactly what you are looking for. Click the title to open the link.

### Specific Documents

Please refer to the *Deploying Enterprise-Grade Wi-Fi Telephony* white paper. It covers the security, coverage, capacity and QoS considerations necessary for ensuring excellent voice quality with enterprise Wi-Fi networks.

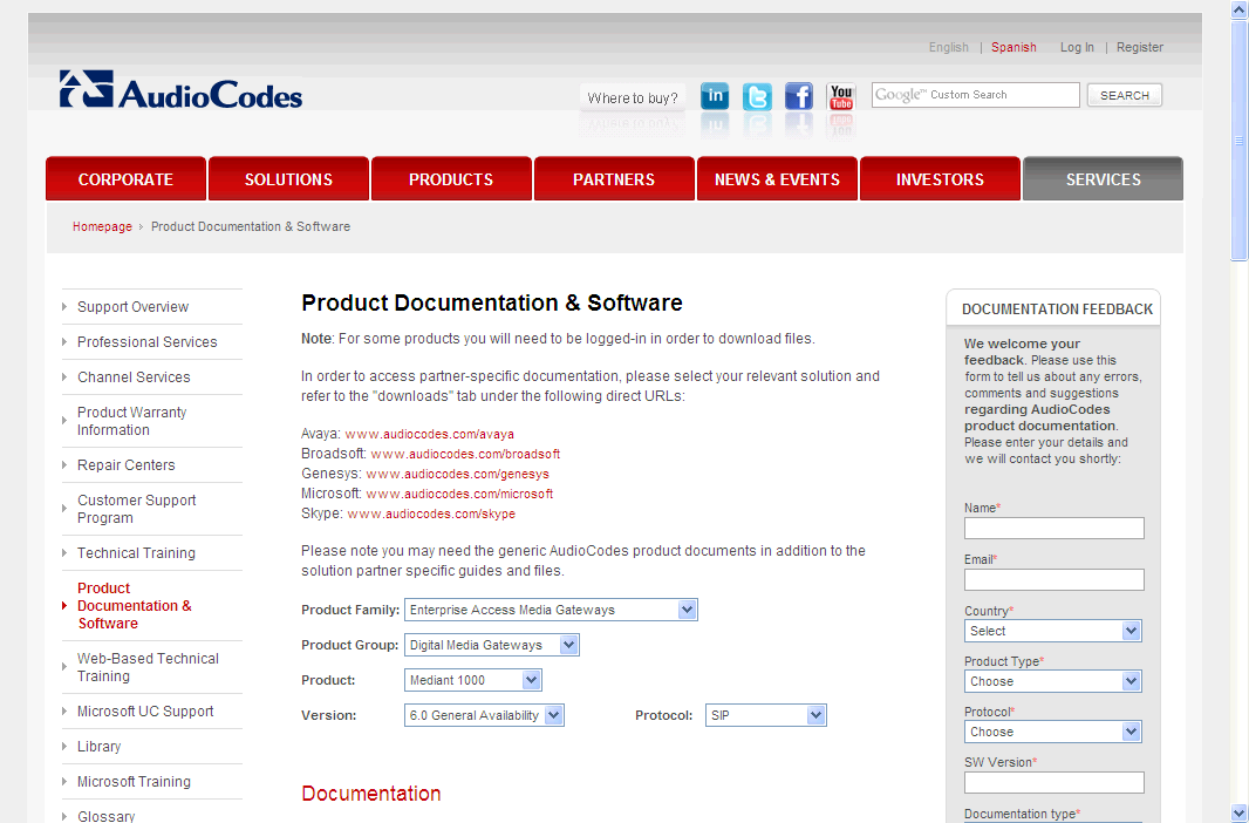
For more detailed information on wireless LAN layout, network infrastructure, QoS, security and subnets, please see the *Best Practices Guide to Network Design Considerations for SpectraLink Wireless Telephones*. This document identifies issues and solutions based on Polycom's extensive experience in enterprise-class Wi-Fi telephony. It provides recommendations for ensuring that a network environment is adequately optimized for use with SpectraLink Wireless Telephones.

Deployment of the SpectraLink 84-Series Wireless Handsets is fully outlined in the *SpectraLink 84-Series Wireless Telephone Deployment Guide*.

*Spectralink 84-Series Wireless Telephone Administration Guide* covers all configuration parameters for the 84-Series Wireless Telephones.

## AudioCodes References

AudioCodes references are available at http://www.audiocodes.com/downloads. Select the options as shown in the next screen to display a list of relevant documents.




**Note: Mediant Gateway**

Throughout this guide, the term *Mediant Gateway* refers to the AudioCodes Mediant 1000.

# Conventions Used In This Document

## Icons

Icons indicate extra information about nearby text.

**Warning**

The *Warning* icon highlights an action you must perform (or avoid) to avoid exposing yourself or others to hazardous conditions.

**Caution**

The *Caution* icon highlights information you need to know to avoid a hazard that could potentially impact device performance, application functionality, successful feature configuration and/or affect handset or network performance.

**Note**

The Note icon highlights information of interest or important information that will help you be successful in accomplishing a procedure or understanding a concept.

**Tip**

The Tip icon highlights information that may be valuable or helpful for users to know, such as special techniques, shortcut methods, or information that will make user tasks easier to perform.

**Web**

The *Web Info* icon highlights supplementary information available online such as documents or downloads on support.spectralink.com or other locations.

**Timesaver**

A time-saving tip is typically used to mention or highlight a faster or alternative method for users who may already be familiar with the operation or method being discussed.

**Admin Tip**

This tip advises the administrator of a smarter, more productive or alternative method of performing an administrator-level task or procedure.

**Power User**

A Power User Tip is typically reserved for information directed specifically at high-level users who are familiar with the information or procedure being discussed and are looking for better or more efficient ways of performing the task. For example, this might highlight customization of a feature for a specific purpose.

**Troubleshooting**

This element can be used in any type of document and is typically used to highlight information to help you solve a relevant problem you may encounter, or to point to other relevant troubleshooting reference information.

**Settings**

The Settings icon highlights information to help you zero in on settings you need to choose for a specific behavior, to enable a specific feature, or access customization options.

## Typography

A few typographic conventions, listed next, are used in this guide to distinguish types of in-text information.

| *Convention* | *Description* |
|---|---|
| **Bold** | Highlights interface items such as menus, soft keys, file names, and directories. Also used to represent menu selections and text entry to the handset. |
| *Italics* | Used to emphasize text, to show example values or inputs, and to show titles of reference documents available from the Spectralink Support Web site and other reference sites. |
| Underlined blue | Used for URL links to external Web pages or documents. If you click on text in this style, you will be linked to an external document or Web page. |
| Bright orange text | Used for cross references to other sections within this document. If you click on text in this style, you will be taken to another part of this document. |
| `Fixed-width-font` | Used for code fragments and parameter names. |

This guide also uses a few writing conventions to distinguish conditional information.

| *Convention* | *Description* |
|---|---|
| <*MACaddress*> | Indicates that you must enter information specific to your installation, handset, or network. For example, when you see <*MACaddress*>, enter your handset's 12-digit MAC address. If you see <*installed-directory*>, enter the path to your installation directory. |
| > | Indicates that you need to select an item from a menu. For example, **Settings** > **Basic** indicates that you need to select **Basic** from the **Settings** menu. |

# Part I: The AudioCodes Solution

Part I introduces you to the AudioCodes Mediant Gateway AudioCodes Mediant Gateway and how it solves the problem of using Spectralink 84-Series SIP endpoints with an Avaya Communication Manager PBX. This solution was tested in the Spectralink labs and the details of the test configuration and its results are covered here.

This Part also guides you through unpacking the AudioCodes Mediant Gateway and preparing it for configuration.

# Chapter 1: Test Overview

The Spectralink 84-Series Wireless Handsets utilize standards-based SIP telephony signaling. In order to deploy these handsets in a facility that uses a legacy non-SIP PBX/call server, a device that converts the signal as it passes between the handset and the PBX is required. This document describes the Mediant Gateway solution and provides guidelines for provisioning the Mediant Gateway and PBX when used in conjunction with an Avaya Communication Manager.

The Mediant Gateway provides a bridge between the Spectralink 84xx wireless handsets and the Avaya Communication Manager—a PBX that offers traditional telephony interfaces such as T1 or E1. The Mediant Gateway transparently manages the protocol translation and interworking between the two systems, enabling deployment of advanced wireless VOIP technology without a complete overhaul of an existing system.

Due to variations in facility systems, many configuration options exist. This document covers the basic setup that was tested in the Spectralink laboratories and demonstrates the workability of this solution. For detailed configuration information as it applies to your facility please refer to the administrative or user manuals of the respective products.

This document does not cover other functionality of the AudioCodes Mediant Gateway , how to configure the Avaya Communication Manager, how to deploy a WLAN or how to configure the Spectralink 84-Series Wireless Handsets for wireless connectivity. These subjects are covered in other documents referenced below.

## *Results Overview*

During the compliance testing, the Spectralink 8440/84580/8452 was able to register as a SIP client endpoint with the Mediant Gateway which routed calls to the Avaya Communication Manager only when PBX call routing was required. The Spectralink handsets were able to place and receive calls routed through the Avaya Communication Manager and also place and receive calls with other 84-Series endpoints through the Mediant Gateway without any PBX involvement. The compliance tests focused on basic telephony features.

### The Test Equipment

The following equipment and software were used during the lab test.

Table 1

| *Equipment* | *Software/Firmware* |
|---|---|
| Avaya Communication Manager | v 5.2 |
| AudioCodes Mediant 1000 w/ SAS option | v 6.20A.054 |
| Spectralink 8440 Handsets | UCS 4.0.2.8017 |

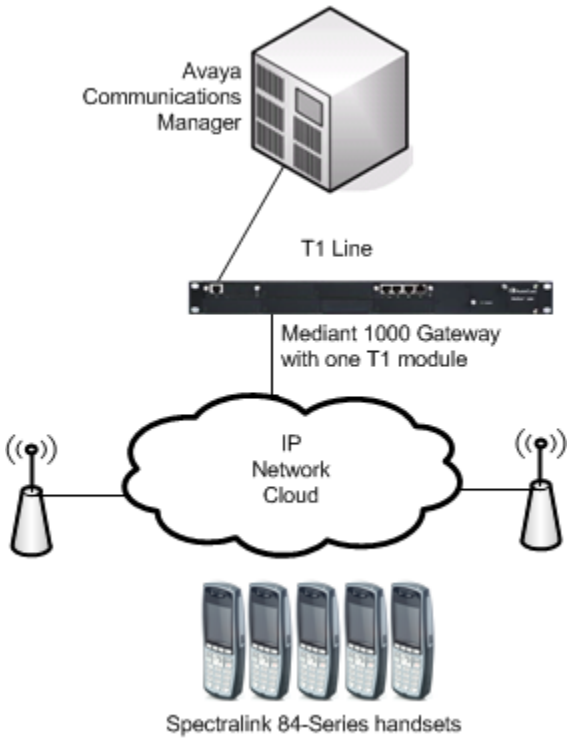
**Admin Tip: Avaya Communication Manager software version supported.**

The test was conducted on an Avaya Communications Manager running version 5.2. However, Spectralink supports this solution on versions ranging from 5.0 to 6.1. The screens and parameters displayed in this document should be similar on all supported versions.

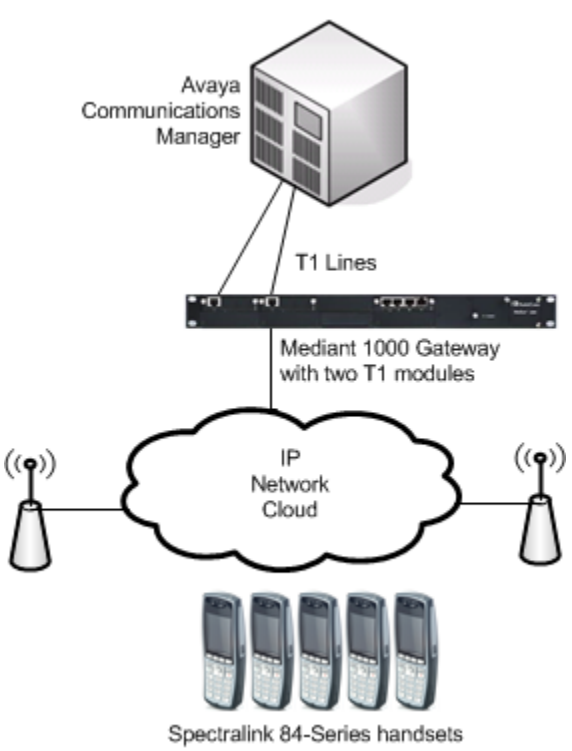
## Network Topology

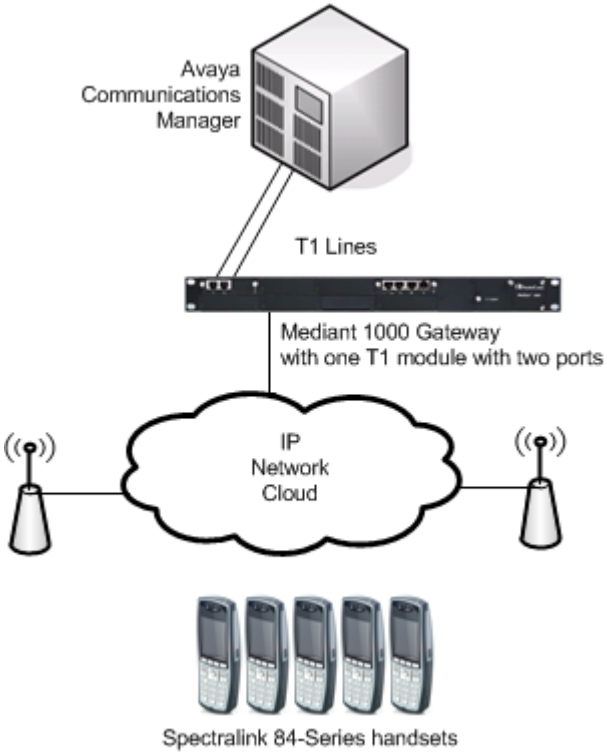
The solution tested at the Spectralink laboratories consisted of an Avaya Communication Manager, an AudioCodes Mediant Gateway, and Spectralink 84-Series handsets. Four different configurations were tested as shown in the following diagrams. The handsets were already operational in the wireless network and that exact infrastructure is not directly relevant to this application note.

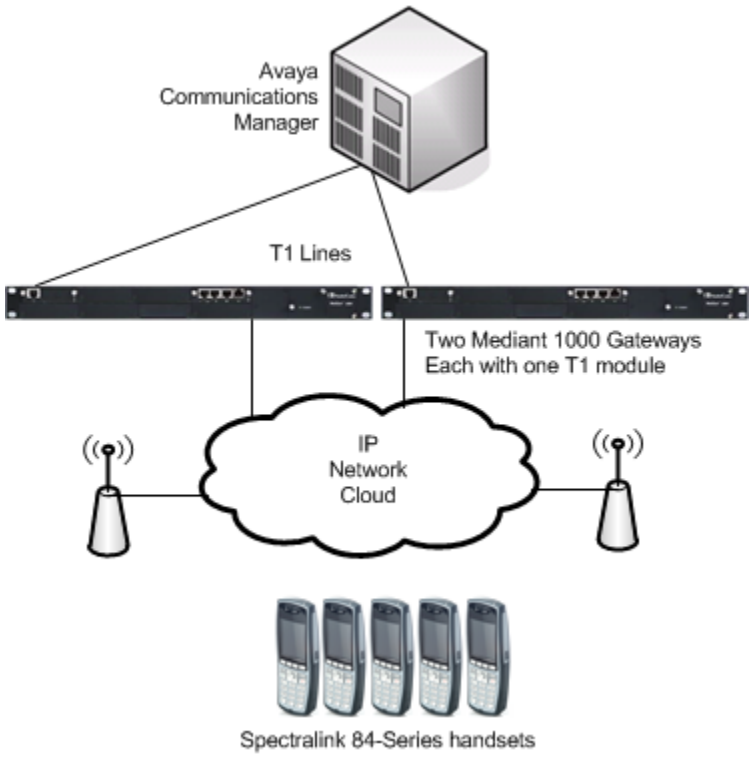
## The basic configuration




## The three expansion configuration options






## Why Q.SIG?

When integrating Spectralink 84-Series handsets with a legacy PBX using the AudioCodes Mediant Gateway, it is vital to select the right line interface between the Mediant Gateway and PBX. The recommended and supported line interface is Q.SIG PRI.

Q.SIG has a richer signaling capability than T1 Channel Associated Signaling (CAS) or Analog line interfaces enabling the broadest telephony feature set on the Spectralink 84-Series handset using the Mediant Gateway solution.

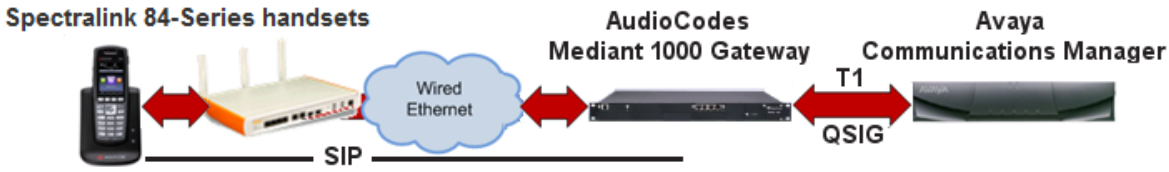
## A Word about Wi-Fi

Many customers install a single wireless network to support both voice and data. Deploying a Wi-Fi network that supports voice is not difficult but there are guidelines that should be followed. Spectralink has documented these best practices and it is important that the wireless network meets these guidelines to achieve user satisfaction.

Although not specifically covered in this document, for optimum performance the deployed access points should conform to the VIEW program as documented in the Spectralink best practices references and listed in the *Spectralink VIEW Certified Products Guide*.

# Chapter 2: What the Mediant Gateway Does

In a typical deployment, the Spectralink 84-Series Wireless Handsets use 802.11 a/b/g/n Wi-Fi with the open-standard Session Initiated Protocol (SIP) for telephony signaling to and from the call server (i.e. PBX). In a facility where the call server does not recognize the SIP protocol, the Mediant Gateway provides protocol translation for smooth call operations. The Mediant Gateway and handsets communicate using SIP and the handsets are configured to register with the Mediant Gateway . The Mediant Gateway communicates with the PBX via the signaling protocol supported by the telephony lines.




Fundamentally, the SIP User Agent in the Spectralink 84-Series Wi-Fi handset must register with a SIP Proxy for operation, and this SIP Proxy must provide routing capability for both outgoing calls from the handsets as well as incoming calls to them. For this solution, a SIP Proxy within the Mediant Gateway serves this role. This proxy is a component of a feature called Standalone Survivability (SAS). The primary application of SAS is to provide routing capability to SIP handsets that register to a Hosted SIP Proxy when connectivity to that SIP Proxy becomes unavailable.

In our application of this feature, the Mediant Gateway is configured for continual SAS operation and the Mediant Gateway permanently operates in Standalone Mode with its local SIP Proxy enabled.

The Mediant Gateway creates a database of user Registrations as handsets contact the Mediant Gateway. It uses this database to function as a local SIP Proxy and facilitate user-to-user calls.

On the other side of the translation, the Mediant Gateway operates as a PRI gateway providing connectivity to the PBX.

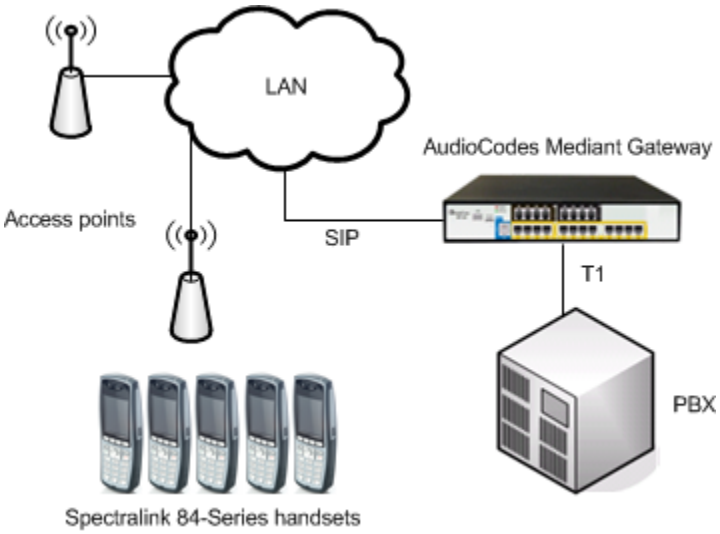
Consequently, configuration options for the SAS component and the PRI component of the Mediant Gateway must be configured.

# How Stand Alone Survivability Application Works

The SAS application is an optional capability of the Mediant Gateway but is mandatory for the Spectralink solution. It is a robust solution originally designed for system redundancy but this document only describes its application to the Spectralink solution.

## SAS Emergency State

The Spectralink Mediant Gateway solution operates the SAS application, permanently, in the Outbound Proxy mode in the emergency state. This means Spectralink SIP handsets use the Mediant Gateway SAS application as a proxy and calls are routed via the Mediant Gateway trunk to the PBX.




When the Mediant Gateway receives calls from a SIP device, it searches its SAS registration database to locate the destination address (according to AOR or Contact). If the destination address is found in the SAS registration database, the call is placed to the other SIP device and no PBX functionality is required. If the destination address is not found, i.e. it is not another SIP device registered on this Mediant Gateway, the SAS application forwards the call to the core Mediant Gateway application, which in turn routes the call across the TDM trunk to the PBX.

## User Authentication

Access to the Mediant Gateway from the Wi-Fi handsets is screened by the security mechanisms of Wi-Fi access points.

Basic SAS functionality does not authenticate users. It accepts all valid registrations which would theoretically allow one handset to emulate a different one.

# Chapter 3: Features and Capacity

## System Capacity Requirements

There are several relevant capacity metrics that must be determined before determining what resources are required in the type of system we have tested – the number of users, the number of simultaneous connections required to the PBX, and the various call configurations that are used in any particular facility.

The number of users is straightforward – how many simultaneously registered users are required? Multiple users of a single wireless handset that are never registered at the same time do not need to be factored in – just the maximum number of simultaneously registered users.

The next relevant metric, the number of simultaneous connections required to the PBX is not so easily calculated. A dedicated voice channel is not required for every user since all of the users would likely never be connected to the PBX at the same time in the same way that all the PBX users would be unlikely to be connected at the same time. Although endpoints registered to a single Mediant Gateway will not need a PBX channel when calling another endpoint registered to the same Mediant Gateway, a multiple Mediant Gateway system will require PBX channels to place calls between phones registered to different Mediant Gateways.

The third measurement to consider is the number of endpoint to endpoint calls to/from handsets registered to a single Mediant Gateway . We have seen that the Mediant Gateway will directly connect locally registered Spectralink 84-Series handsets with each other and this type of call does not require connection through a PBX. In some environments this type of call could be the most prevalent. In other facilities, we would expect heavier use of a PBX. Every installation is unique and must be evaluated accordingly.

## Capacity Analysis

The Mediant Gateway can support up to 600 handsets on the SIP side of the system. This means that if all calls were placed only between SIP handsets, 300 simultaneous calls would be possible. However, the T1 trunk has 23 channels and this is the limiting factor when calls are routed through the PBX. Each call uses at least one of these channels, and if multiple lines are deployed, then one handset could potentially utilize as many channels as it has lines. Therefore any analysis of capacity requirements must study the ratio of the endpoint-to-endpoint usage against the demands that will placed upon the PBX and the T1 line.

Multiple PRIs installed in the Mediant Gateway solve the capacity issue to some degree. Each T1 module can support up to four T1 trunks and each Mediant Gateway can support up to four T1 modules, but the number of PRIs is limited to four therefore the capacity of any single Mediant Gateway is 92 channels.

Additional Mediant Gateway s can be added to increase capacity using the same formula as above.

In almost every scenario, the trunk interface voice channels should not have a 1:1 mapping with telephony extensions. Instead the trunk interface is configured to dynamically support more SIP end points than the actual channels. In fact, tying channels to specific extension is undesirable as it prevents features requiring more than one active line such as transfer, forward, hold, etc.

Typical business handset usage during busy hours requires somewhere between 0.1 and 0.2 voice circuits per user/extension to the PBX. In other words each voice channel to the PBX from the Wi-Fi handset users can support between 5 and 10 users. In more traditional telephony terms, each user requires between 100 and 200 milli-Erlangs of capacity to the PBX. Using the 100 milli-Erlang calculation, 230 handsets could be supported per T1 PRI (which has 23 voice DS0 channels). Each Mediant Gateway has a simultaneous registration maximum of 600 so here again the usage factor is critical to accurate deployment capacity.

## Features Tested and Validated

The Spectralink 84-Series handsets are state of the art SIP endpoints. The extensive feature set and configuration possibilities create a custom telephony environment only available within the SIP protocol. Many of these features, if not most, are available within this solution. However some features do not survive the translation from one protocol to another and cannot be expected in this hybrid environment. See the table on the next page and the footnotes that follow.

| ***Handset Features*** [1] | ***Mediant Gateway*** | ***SIP*** |
|---|---|---|
| Incoming/Outgoing calls [2] | Y | Y |
| Call waiting | Y | Y |
| Caller ID [3] | Y | Y |
| Codec: G.711, G.729 | Y | Y |
| Conference: 3-way | Y | Y |
| Do not disturb | Y | Y |
| Forward: busy, no answer, and manual | Y | Y |
| Hold and Resume [4] | Y | Y |
| Registration | Y | Y |
| Transfer: blind and attended [3] | Y | Y |
| Up to 6 call appearances per line [5] | Y | Y |
| Speed dial [6] | Y | Y |
| Contacts/Directory | Y | Y |
| User Profiles | Y | Y |
| Lines per phone | Y | Y |
| Redial | Y | Y |
| Call history | Y | Y |
| Distinctive ring | Y | Y |
| PTT | Y | Y |
| OAI | Y | Y |
| XML API applications | Y | Y |
| Exchange calendar integration | Y | Y |
| IM | Y | Y |
| SIP URL calls | Y | Y |
| Speaker and Mute | Y | Y |
| Paging (off-PBX/84-Series handsets-only) | Y | Y |
| Voicemail | N | Y |
| Message waiting indication | N | Y |
| PBX-based features [8] | N | Y |
| ‘Paired’ lines (shared line, bridged line, etc. – ‘ring both phones’ generally) | N | N |
| Music on hold [4] | N | Y |
| Hold recall | N | Y |
| Park/Pickup/Directed Pickup | N | Y |
| Busy lamp field | N | Y |

| ***Handset Features*** [1] | ***Mediant Gateway*** | ***SIP*** |
|---|---|---|
| Camp-on (“automatic callback”) | N | Y |
| Authentication | N | Y |
| Hunt groups | N | Y |
| Group paging (integrated with PBX) [8] | N | Y |
| Call Park | N | Y |
| Distinctive Ring | N | Y |
| HD Voice (Siren Codec) | N | Y |
| Per Line Authentication | N | Y |

## Footnotes

1. Core Features

   Core Features reside locally in the handset but require some interaction with the Mediant Gateway and PBX. These features work only as long as the phone is registered and turned on.

   If the phone is turned off, registered to a different user or moves out of range for an extended period of time, calls to the handset are neither received nor forwarded. When the phone is unavailable, the Mediant Gateway must provide a fallback option for how to handle these calls. We specify where to send calls like these in Chapter 6, section 12. Configure IP to Trunk Routing.

2. Incoming/Outgoing calls

   Incoming/Outgoing calls include to/from another 84-Series handset, a (TDM or proprietary VoIP) desk phone, and a trunk.

   What happens during the timeout?
   Necessarily, we have to set a time period for the Mediant Gateway to realize that the handset is not available. Any timeout creates a window of time where the phone could be turned off or out of range during which calls that come to it will not respond in the usual way. The caller will hear only silence, not a busy tone or a ring. Too short a timeout will over-burden the Mediant Gateway with repeated registration requests. In this document we have recommended a 60 second timeout with the understanding that sometimes the phone will give an unexpected response to a caller during this 60 second window.

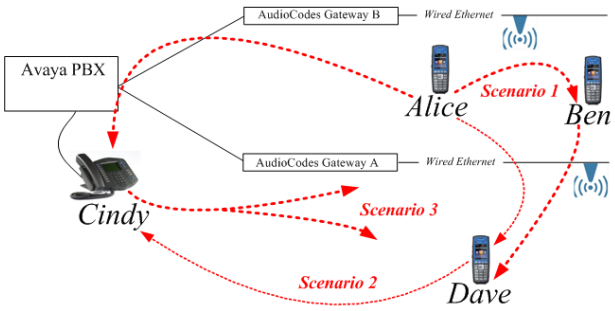
3. Caller ID display during call transfers

   Caller ID can be confusing during call transfers. Let’s look at three scenarios while referring to the diagram below in which Alice and Ben have 84-Series handsets on the same Mediant Gateway , Dave has an 84-Series handset on another Mediant Gateway , and Cindy has a deskphone.

Scenario 1: Alice calls Ben, who transfers the call to Dave. When the transfer is complete Dave's phone will see Ben's caller ID (not Alice's) displayed on his screen. Alice's phone will show that she is talking to Dave.

Scenario 2: Alice calls Dave, who transfers the call to Cindy. When the transfer is complete Alice continues to see Dave's caller ID (not Cindy's) displayed on his screen. Cindy's phone works as expected, displaying Alice's caller ID.

Scenario 3: Alice calls Cindy, who transfers the call either to Ben or to Dave. When the transfer is complete, Ben or Dave then see Cindy's caller ID (not Alice's) displayed on his screen. Alice also still show's Cindy's Caller ID.




4. Music-on-Hold

   The Mediant Gateway does not provide music on hold or periodic tones to a caller placed on hold. If a PBX station places an 84-Series phone attached to the Mediant Gateway on hold music on hold will be heard if the PBX is configured to provide it.

5. Calls per line

   "Calls per line" is an underlying capability needed for several of the above features, but is not considered a feature in its own right.

6. Speed dial

   Speed dial is configured locally at the 84-Series handset – PBX configured speed dial, for groups for example, are listed separately.

7. Contacts/Directory

   Contacts are configured locally at the 84-Series handset – PBX configured Directory is listed separately.

8. PBX-based features

   PBX features include: forward, conference, transfer, do not disturb, system/group speed dials)

# Chapter 4: Unpacking and Familiarizing Yourself with the Mediant Gateway

## Package Contents

Mediant Gateway shipments arrive with a large box for the Mediant Gateway and power cable and a smaller package containing the T1 module.

You will need to supply Ethernet cables and a T1 crossover cable for each T1 module deployed.

### Front-Panel Description

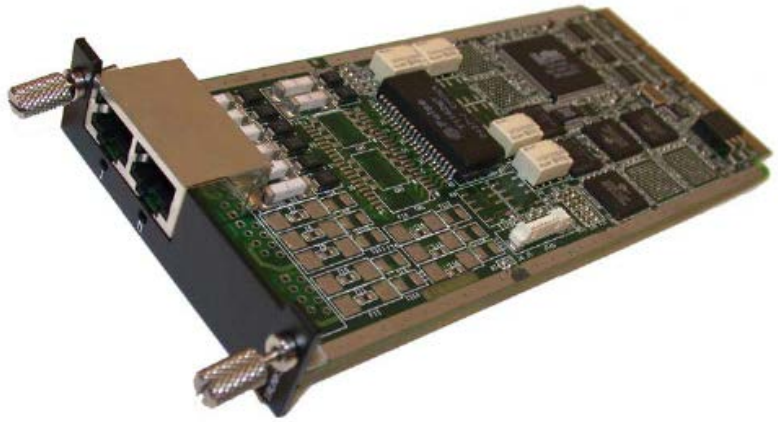
| *Item #* | *Label* | *Description* |
|---|---|---|
| 1 | T1 | Telephony modules. |
| 2 | CRMX or CMX | Hosts either the CRMX module (for data routing) or the CMX module (CPU for VoIP Mediant Gateway functionality) |
| 3 | Power 1 | (Optional) Spare Power Supply module slot |
| 4 | Power 2 | Main Power Supply module |
| 5 | - | Extractable Fan Tray module with a schematic displayed showing the chassis' slot numbers |

## T1/E1 Module

The chassis supports up to four digital E1/T1/J1 modules. The module is available in 1-, 2-, or 4-span configurations, providing RJ-48c ports (not RJ45). The ports are labeled I, II, III, and IIII. The maximum number of ports that can be utilized is four.

**Note: T1 Module**

The T1 Module is shipped separately from the chassis.



Each port provides a LED that indicates operating status.

| *Color* | *State* | *Description* |
|---|---|---|
| Green | On | Trunk is synchronized (normal operation) |
| Red | On | Loss due to:<br>LOS – Loss of Signal<br>LOF – Loss of Frame<br>AIS – Alarm Indication Signal (the Blue Alarm)<br>RAI – Remote Alarm Indication (the Yellow Alarm) |
| - | Off | Failure or disruption in the AC power supply or the power is currently not being supplied to the device through the AC power supply entry. |

## CRMX Module

The single CRMX Module supports data routing, switching, security, and voice security (SBC) capabilities. The module provides three LAN ports, a WAN port (not used in this deployment) and an RS-232 interface port.

**Note: CRMX Module**

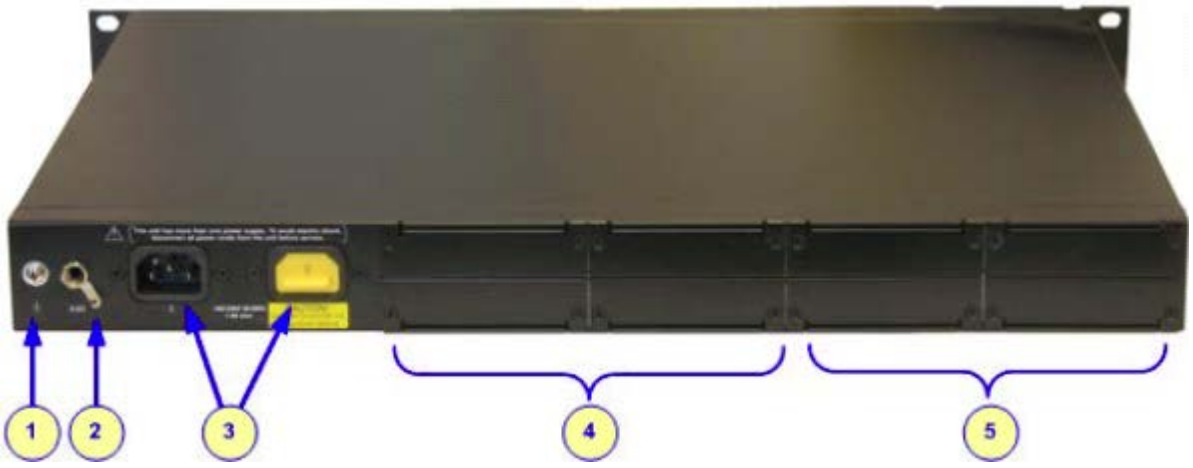
The CRMX Module is installed in the chassis.

| *Label* | *Component Description* |
|---|---|
| I, II, III | 10/100/1000Base-T Ethernet LAN ports for connecting computers and/or switches |
| \|0\|0 | RS-232 port for accessing the CLI. A 9-pin DB adaptor cable is supplied. |
| - | Reset pinhole button for resetting the device and restoring the device to factory defaults. See Resetting the Mediant Gateway . |
| 0/0 WAN | WAN Interface (not used in this deployment) |

The LAN ports provide a LED that indicates operating status.

| *Color* | *State* | *Description* |
|---|---|---|
| Green | On | Ethernet link established |
| | Flashing | Data is being received or transmitted |
| | Off | No Ethernet Link |

## Rear-Panel Description




| *Item #* | *Label* | *Description* |
|---|---|---|
| **1** | ⏚ | Protective grounding screw. |
| **2** | ESD | Electrostatic Discharge (ESD) socket. |
| **3** | 100-240V~1A | Dual AC Power Supply Entries. |
| **4** | - | Slots for housing optional components (not used in this deployment) |
| **5** | - | Slots reserved for future use. |

# Chapter 5: Preparing the Mediant Gateway for Initial Configuration

The Mediant Gateway must be configured with a direct connection to a provisioning computer before being connected to the LAN.

## *Insert the T1/E1 Module*

The T1/E1 module is shipped separately and must be installed. Clear Kapton tape covers the gold edge of the module and protects the module's BUS line. It must be removed before the module is inserted into the chassis.

**Warning: Remove the Kapton tape**

If the Kapton tape is not removed, the module will not function and irreversible damage may be caused to the chassis.

**Installing the T1 module into slot one:**

1. Ensure the Kapton tape is removed.
2. On the device's front panel, using a Phillips screwdriver, remove the black metal cover plate protecting the module slot.
3. Insert the required module into the empty slot (use slots 1-5 for the T1 module), aligning the module with the rails in the slot in the following module orientation depending on whether you are inserting it in the top- or bottom-row slots:
   - Top-row slots: ensure that the module is orientated such that the port number labels are located at the bottom of the module's front panel. This module orientation is considered as facing up.

- Bottom-row slots: ensure that the module is orientated such that the port number labels are located at the top of the module's front panel. This module orientation is considered as facing down.

4 Push the module into the slot and press on it firmly to ensure it has been fully inserted.

5 Using a flathead screwdriver, tighten the module's mounting pins.

## Connect to Power
## Connect to Computer

**Warning: Do not connect the Mediant Gateway to the network**

Do not connect the Mediant Gateway to your corporate network before configuring it.

**Connect the Mediant Gateway to the power supply:**

- On the device's rear panel, connect the left (active) 100-240V~50-60 Hz power socket to a standard electrical outlet using the supplied AC power cord.

**Connect the Mediant Gateway to the PC to be used for initial configuration:**

- Use your own network cable to connect the PC (or laptop) network port to a LAN port on the CRMX module.

# Part II: Configuring the Components

Part II covers the steps to configure the Mediant 1000, testing the handsets against the configuration, and installing the Mediant Gateway in its permanent location. Configuration requirements of the Avaya Communication Manager are then covered in detail.

Some facilities may require additional capacity and expanding the system to increase capacity is covered in Chapter 10 Expanding your System.

# Chapter 6: Initial Configuration of the Mediant Gateway

This chapter describes the procedure for initial configuration of a Mediant Gateway (Mediant Gateway ) running software version 6.20.

The default Mediant Gateway username and password is **Admin** and **Admin** respectively, this is required when web-browsing to the Mediant Gateway . Instructions for changing it are in the last section of this chapter.

**Caution: Backup your configuration**

Save and backup your configuration when you complete the configuration steps below.

## *1. Connect Mediant Gateway to a single computer*

**Warning: Do not connect the Mediant Gateway to the network**

Do not connect the Mediant Gateway to your corporate network before configuring it per the instructions in this chapter.

1 Establish a connection between the Mediant Gateway and a single computer or laptop. By default the Mediant Gateway has the following settings:

| | |
|---|---|
| IP Address | 192.168.0.1 |
| Sub net | 255.255.255.0 |

2 Change the Network Config of the pc to match the Mediant Gateway 's default network settings i.e. 192.168.0.100, 255.255.255.0.

3 Open a browser and enter the IP address of the Mediant Gateway **http://192.168.0.1**.

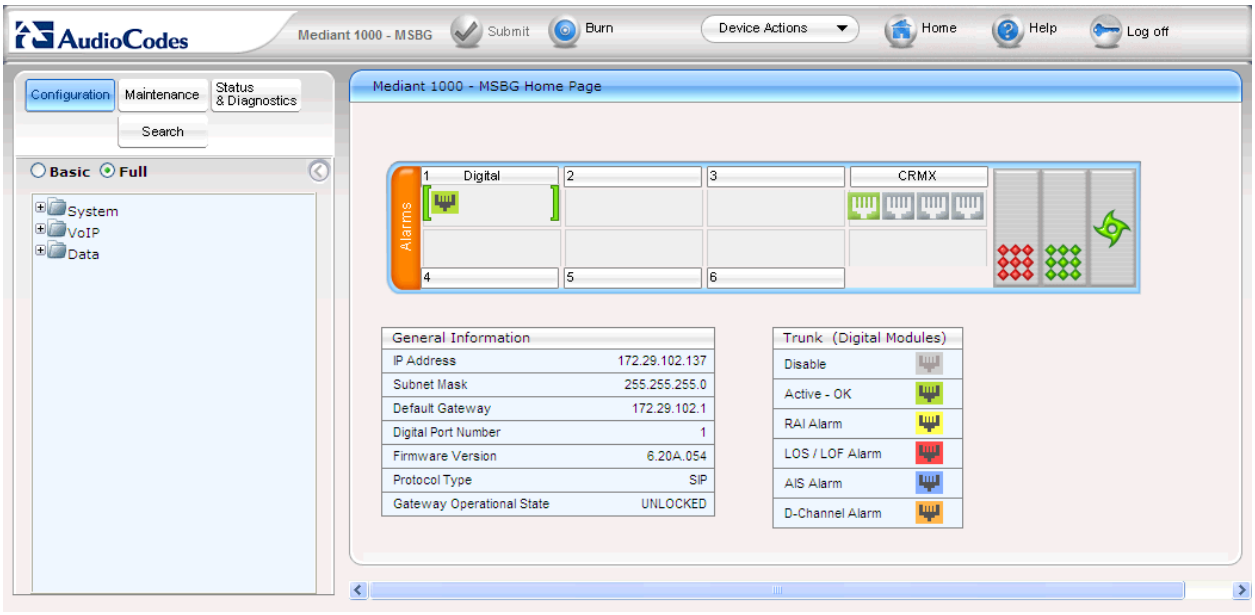
4 When prompted, enter the default username **Admin** and password **Admin**. Note the capital A.

## The Home screen

The Home button opens the Home screen which displays information you may need as you proceed with configuration steps. The below example shows a configured Mediant Gateway . For more information about the Home screen, see the User Guide.

The Home page shows the status of Mediant Gateway components. Any component of the simulated product image can be clicked to display operational information or additional configuration options.

Verify the Firmware Version is 6.20A.054. If it is not this specific version, follow the Software Upgrade Procedure in Appendix B: Software Upgrade Procedure.




## The Toolbar and Navigation pane

Elementary functionality is accessed through the toolbar along the top of the interface and the navigation pane along the left.

## The Burn button

The Burn button writes configuration changes to flash memory. Do this periodically so that you do not lose your work due to a power outage or other system problem.

## Navigation Pane

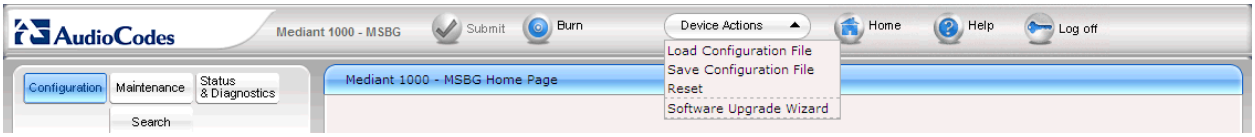
The Navigation Pane on the left side of the window provides the menus to the screens you see illustrated in this document. Ensure that the Full radio button is selected so that you can see all available options.

### The Search option

You can find settings by searching with the Search button located on the Nav pane.

### Device Actions

Use the Reset option on the dropdown menu to reset the Mediant Gateway and activate configuration settings. Certain settings require a reset of the Mediant Gateway to take effect and these are marked with a lightning bolt icon. The Device Actions menu is also where you will find the Software Upgrade Wizard.




**Admin Tip: When do you have to reset the Mediant Gateway?**

If you see a bolt symbol next to an option, it means that the Mediant Gateway has to be reset before that option takes effect.

# 2. Feature Key/License Verification and Upgrade

Ensure you have the features required for Mediant Gateway implementation. Upgrade as needed.

### Verify License keys feature

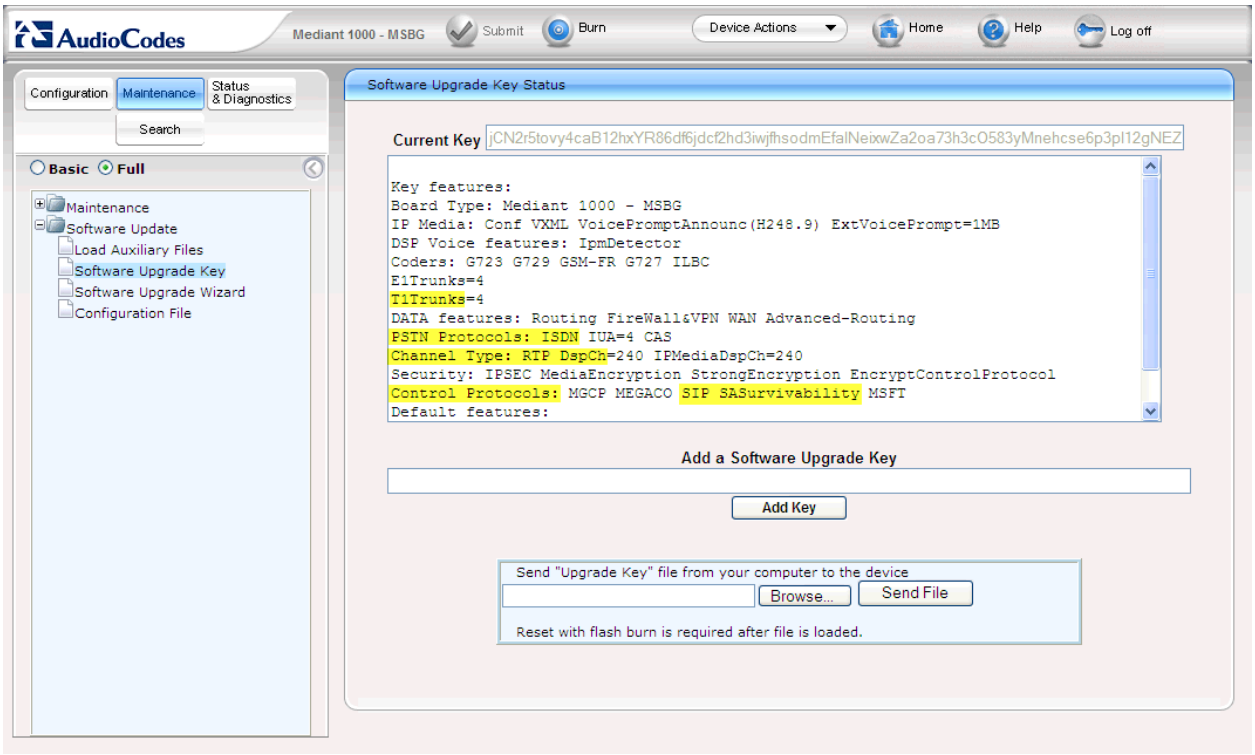
1. Click **Full** to expand the list of drop down menu options
2. Using your web browser log into the Mediant Gateway , select the **Maintenance** tab>Software Update>Software Upgrade Key.
3. Select **Software Upgrade Key.**

Minimum requirements for the License

| | |
|---|---|
| PSTN Protocols | ISDN |
| T1/E1Trunks | 1 |
| Channel Type | RTP DspCh=31 |
| Control Protocols | SIP SASurvivability |

If you do not have this minimum feature key, contact the Spectralink support number.

Example (the screen shown includes more features than the minimum).




## Add Software upgrade key (optional if key needs to be installed)

You will get a file from your representative that will look something like this:

```
[LicenseKeys]
;Run Id  =  142251
;BoardType=Mediant1000
S/N3593541 =
okRqr5topD458Btxxzw3814Zlid5cOda9gZzlhYg9j8aaRd1hSA4aiY3mOjaL2lc80MfeufIxxx
qvGatewayq4PQba2celOF4cyB4rQceeeLA9j8ealJ9YZQba388ni15cOlc80M4f9uocykfa5Ne4
PQ5az8un26WeOSTSM00
```

Your key will look different than the one above. Your key is encrypted with the serial number of the Mediant Gateway you are using. Each Mediant Gateway will require its own key.

Once you get a file with the correct key,

1. Copy the key and paste it into the **Add a Software Upgrade Key** field (key highlighted in yellow).
2. Press the **Add Key** button.
3. The key content appears in the display window. Verify the key content meets the minimum requirements.
4. Use **Device Actions** to Reset the Mediant Gateway .

# 3. Disable DHCP Client and Server

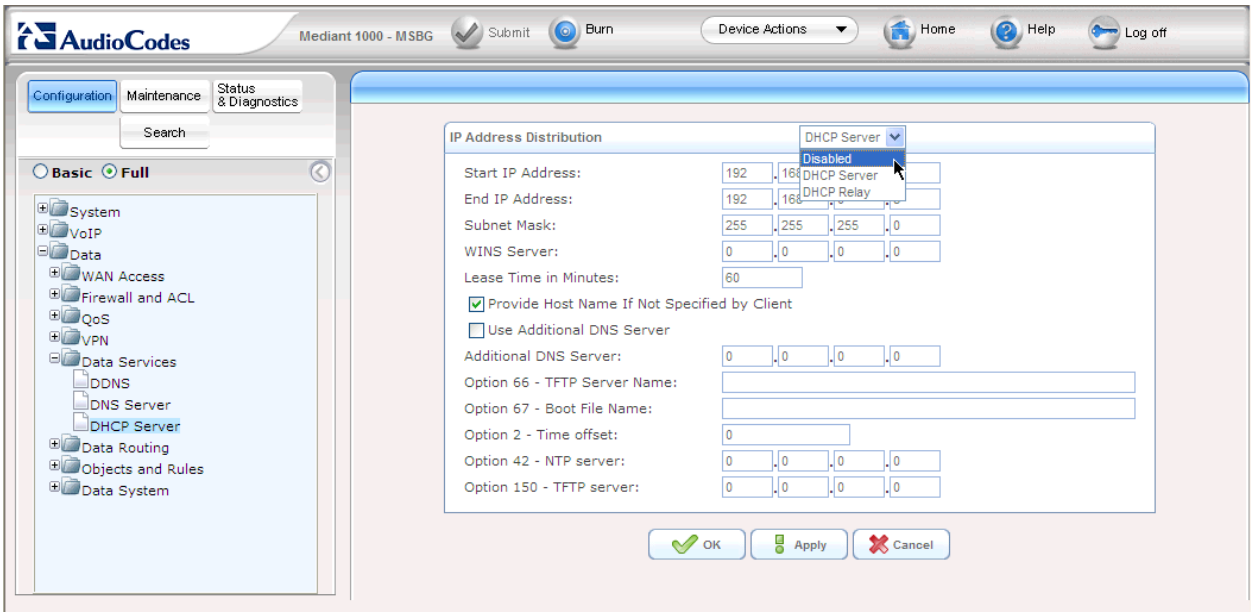
## Disable the Device's DHCP Server

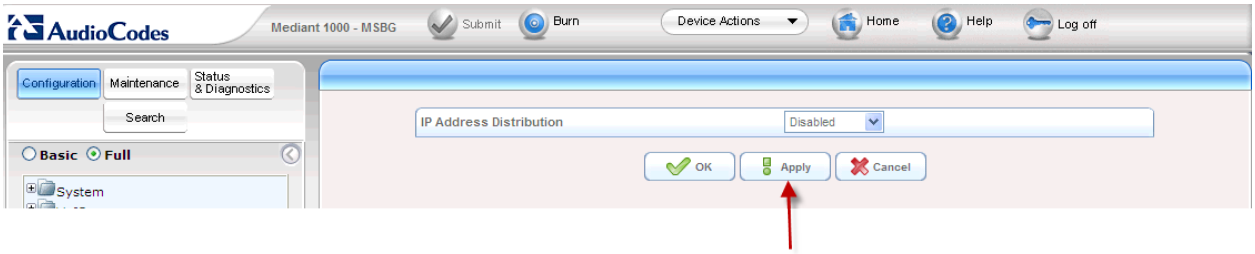
In order to avoid conflict with another DHCP server, during this initial configuration you must disable the DHCP server.

1 Select the Configuration tab and navigate to Data > Data Services > DHCP Server.

2 If **Enabled**, click the pencil icon to edit the settings.

3 Click the down arrow as shown below and select the **Disabled** option. Click **OK**.

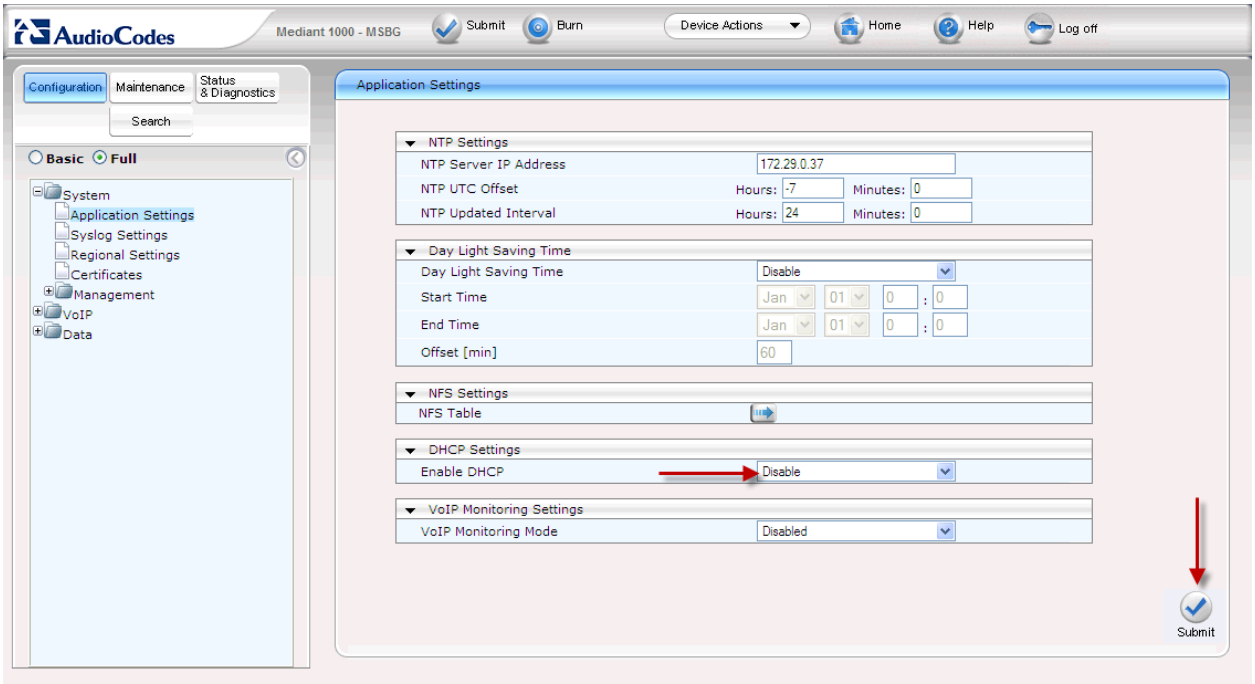



4 Click Apply and Burn.

## Disable the DHCP Client

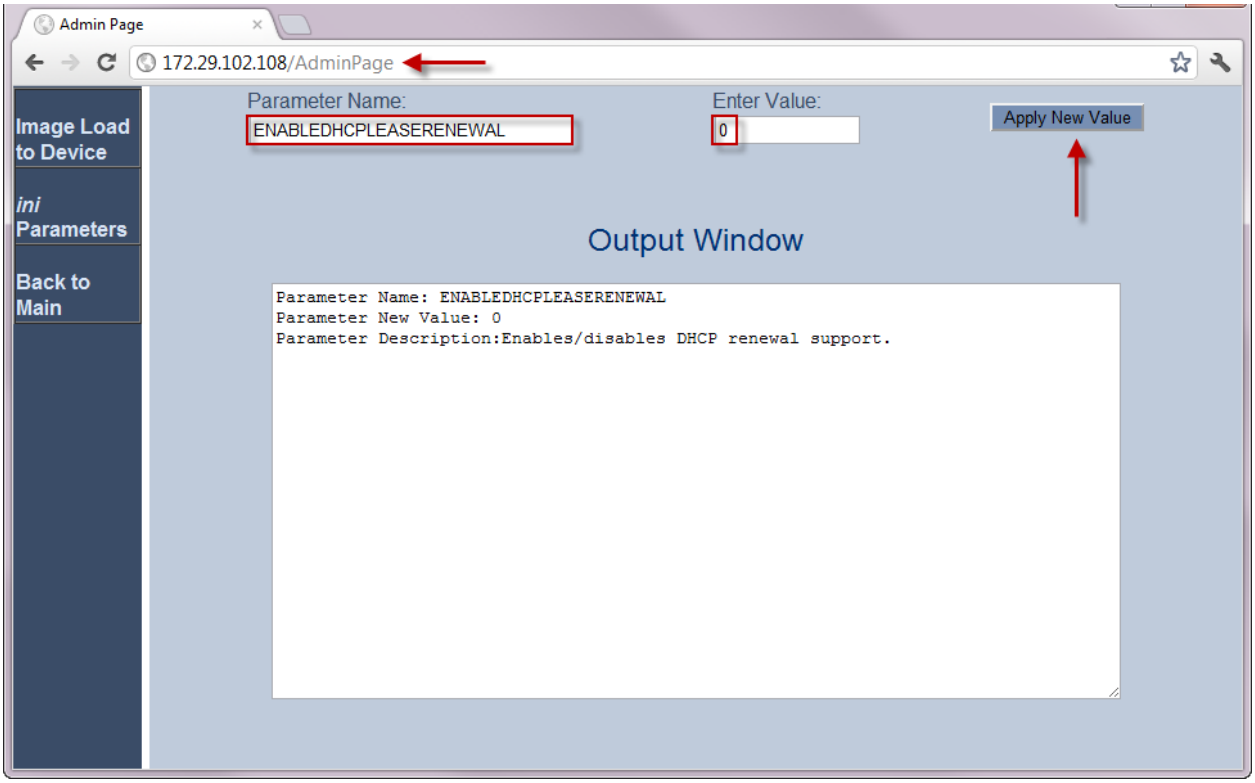
1. Select the Configuration tab and navigate to System > Application Settings.
2. Under DHCP Settings > Enable DHCP select **Disable**.
3. Click **Submit**.



## Set DHCP Lease Renewal

Ensuring this value is set to zero in the Admin Page ensures that the system will not erroneously change it to something else during upgrades.

1. Enter **AdminPage** after the IP address in the browser as shown in the screen below.
2. Select *ini* Parameters in the Nav pane on the left.
3. Enter **EnableDHCPLeaseRenewal** and the value **0**. The entry is case sensitive so enter it exactly as written here. It will convert to all caps as shown in the screen below.
4. Click **Apply New Value**.



# 4. Set Mediant Gateway IP Address

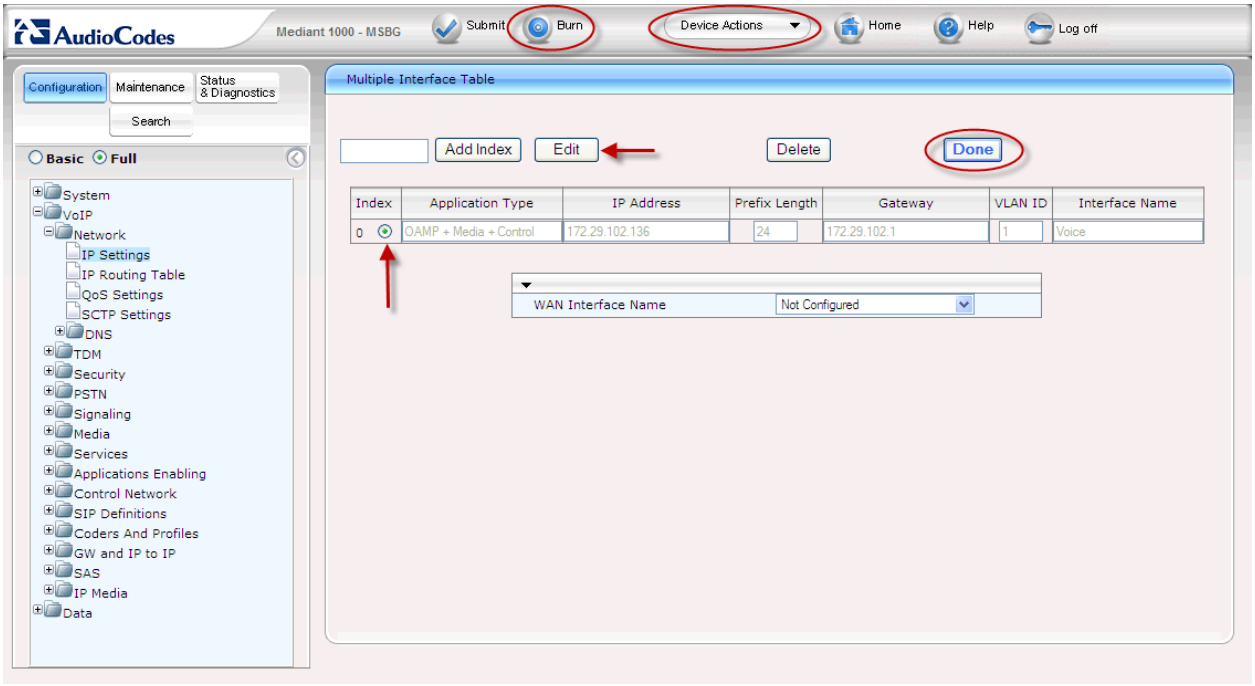
By default the Mediant Gateway has the following settings:

| | |
|---|---|
| IP Address | 192.168.0.1 |
| Sub net | 255.255.255.0 |
| Default Gateway | 192.168.0.1 |

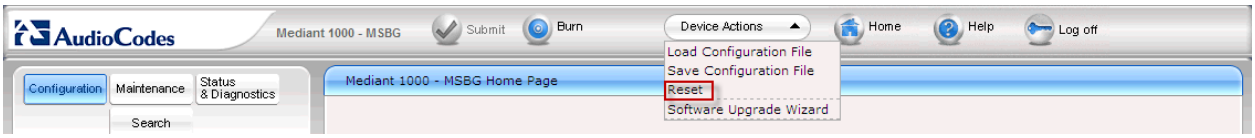
1. Select the Configuration tab and navigate to VOIP > Network > IP Settings.
2. Select the Index to edit by doing one of the following:
   - Click the 0 (zero) Index radio button and then click the Edit button.
   - Add an Index by entering 1 in the box and pressing Add Index.
3. Configure these settings:

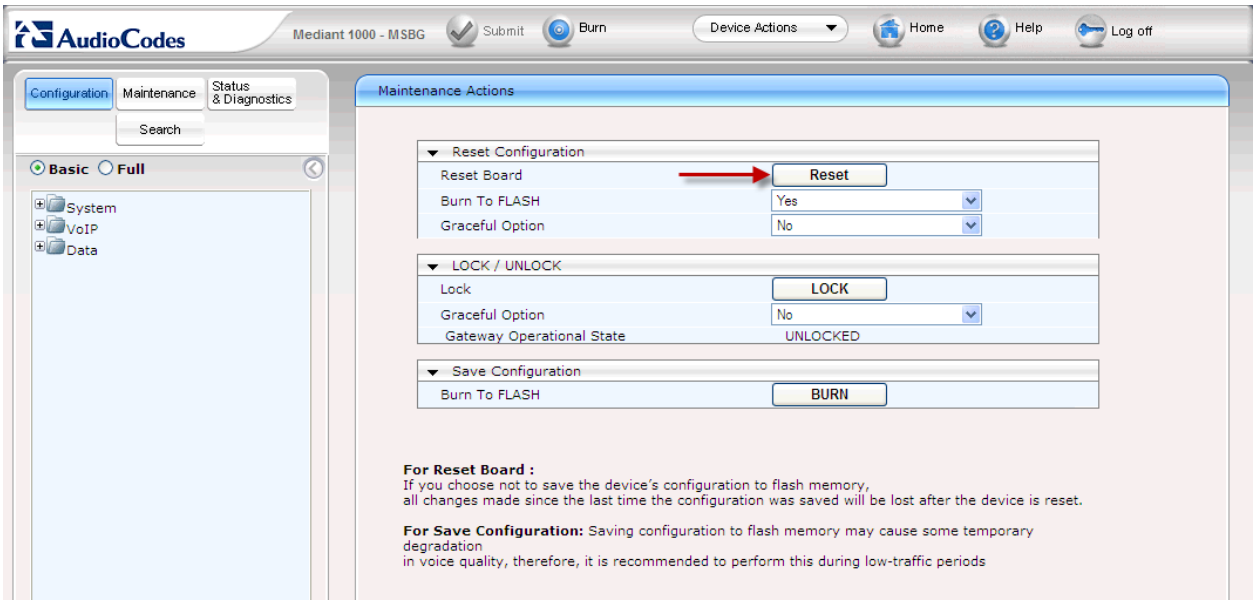
| | |
|---|---|
| Application Type | OAMP+Media+Control |
| IP Address | The Mediant Gateway 's IP address |
| Prefix length | The subnet mask length in CIDR notation |
| Gateway | The default gateway's IP address |
| The VLAN ID | 1 |
| Interface Name | Voice |

4. Click the **Apply** button.
5. Click the **Done** button when finished.
6. Click the **Burn** button.



7 Restart the Mediant Gateway to apply the settings by using the Device Actions dropdown menu and selecting Reset.




8 The Mediant Gateway will reboot and restart using the new IP address.

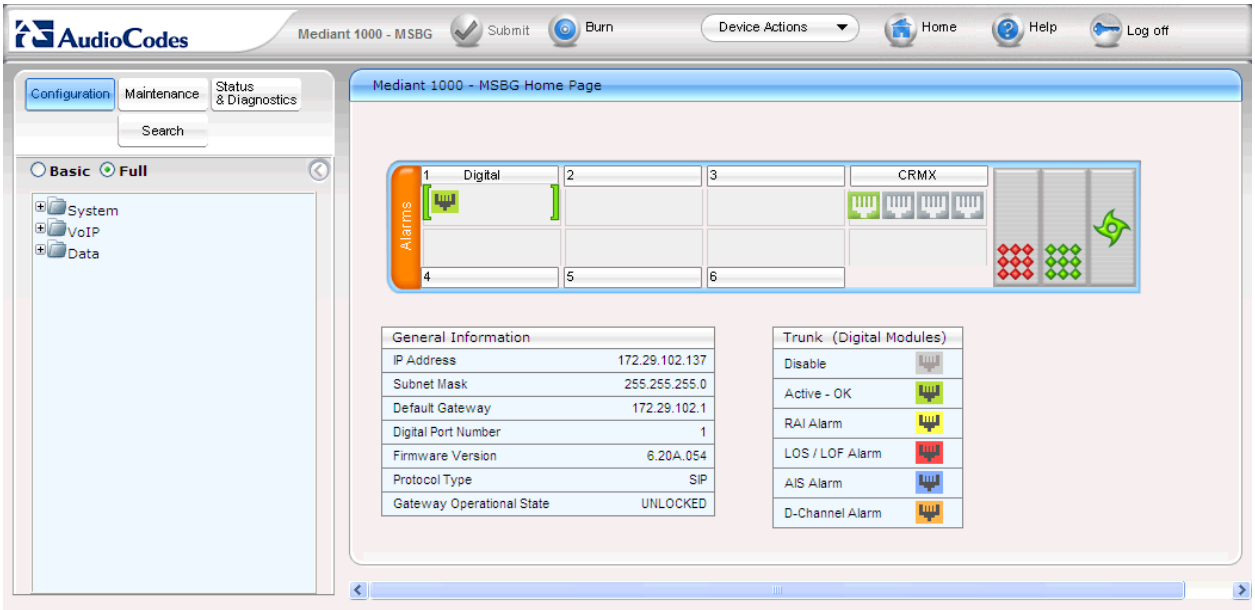
## Verify the settings

1 Log into the Mediant Gateway using your web-browser (changing your PC's IP address to one that will be able to communicate with the gateway's new IP address, if required).

2 Click the **Home** button.

The LAN icon should show green.

Under General Information, double check the IP Address, subnet mask and Default Gateway parameters are as expected.


AudioCodes
Mediant 1000 - MSBG
Submit
Burn
Device Actions
Home
Help
Log off
Configuration
Maintenance
Status & Diagnostics
Search
Basic
Full
System
VoIP
Data
Mediant 1000 - MSBG Home Page
Alarms
1 Digital
2
3
CRMX
4
5
6
General Information
IP Address 172.29.102.137
Subnet Mask 255.255.255.0
Default Gateway 172.29.102.1
Digital Port Number 1
Firmware Version 6.20A.054
Protocol Type SIP
Gateway Operational State UNLOCKED
Trunk (Digital Modules)
Disable
Active - OK
RAI Alarm
LOS / LOF Alarm
AIS Alarm
D-Channel Alarm

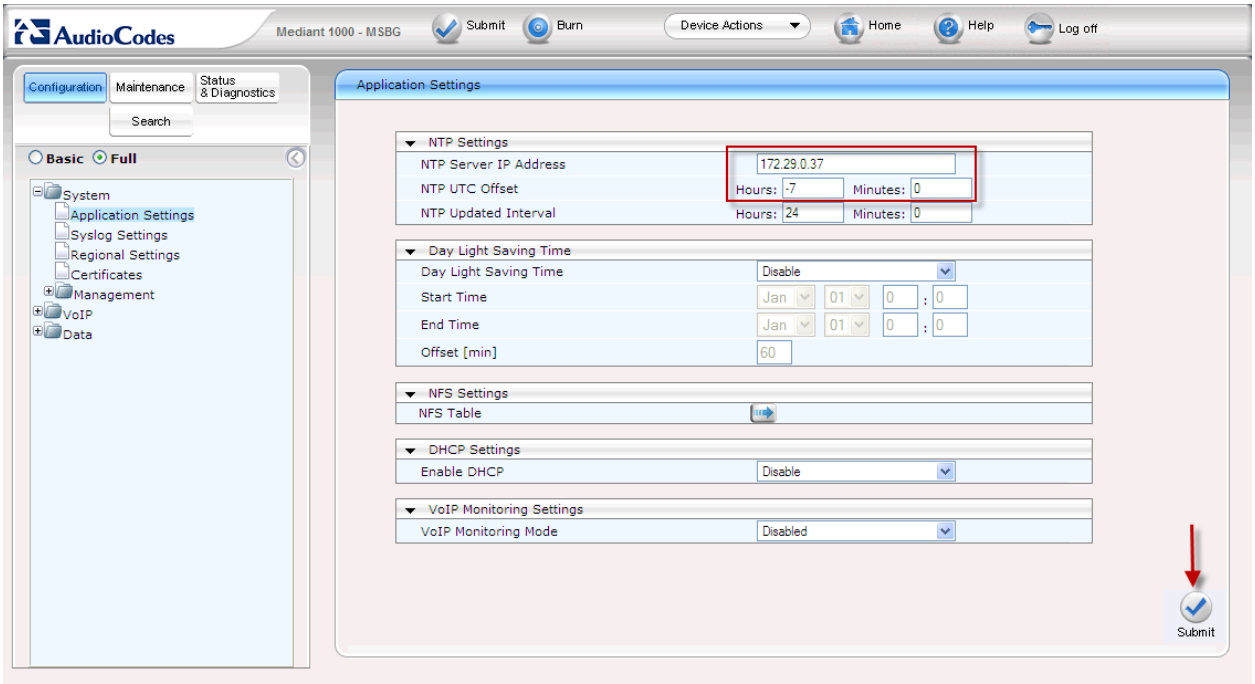
# 5. Set NTP settings

A NTP server will provide necessary time service to your phones, allow the Mediant Gateway to time stamp logs, and assist in any troubleshooting should the need to investigate any issues ever arise.

1 Select the Configuration tab and navigate to System > Application Settings

2 Enter the NTP server IP address.

3 Set **NTP UTC offset** to your local GMT time.




4 Click **Submit**.

# 6. Set Syslog Parameters

Syslog traces are important tools for troubleshooting issues and it is strongly recommended that you have a syslog server set up. The recommended setting allow for maximum logging without sacrificing system quality.

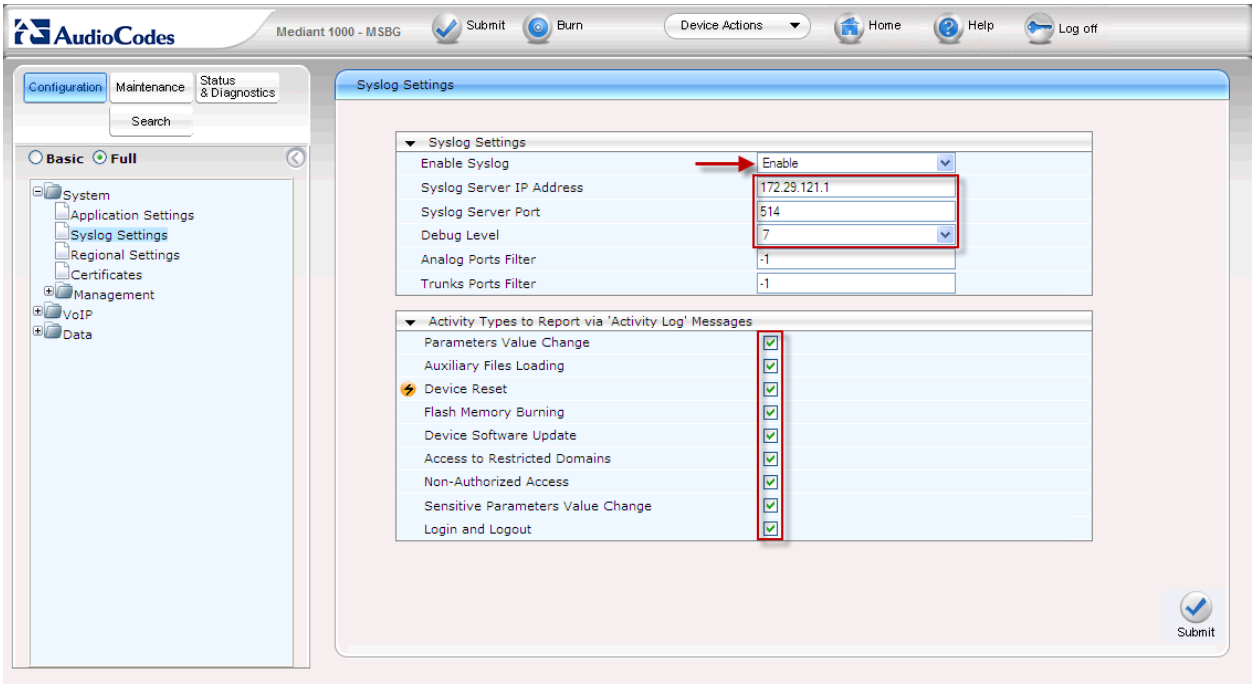
1 Select the Configuration tab and navigate to System > Syslog Settings.

2 Enable Syslog.

3 Set the Syslog Server IP address and the Syslog Server Port. Leave the Port setting at the 514 default.

4 Set Debug Level to 7

5 Ensure all checkboxes are checked as in screen below.

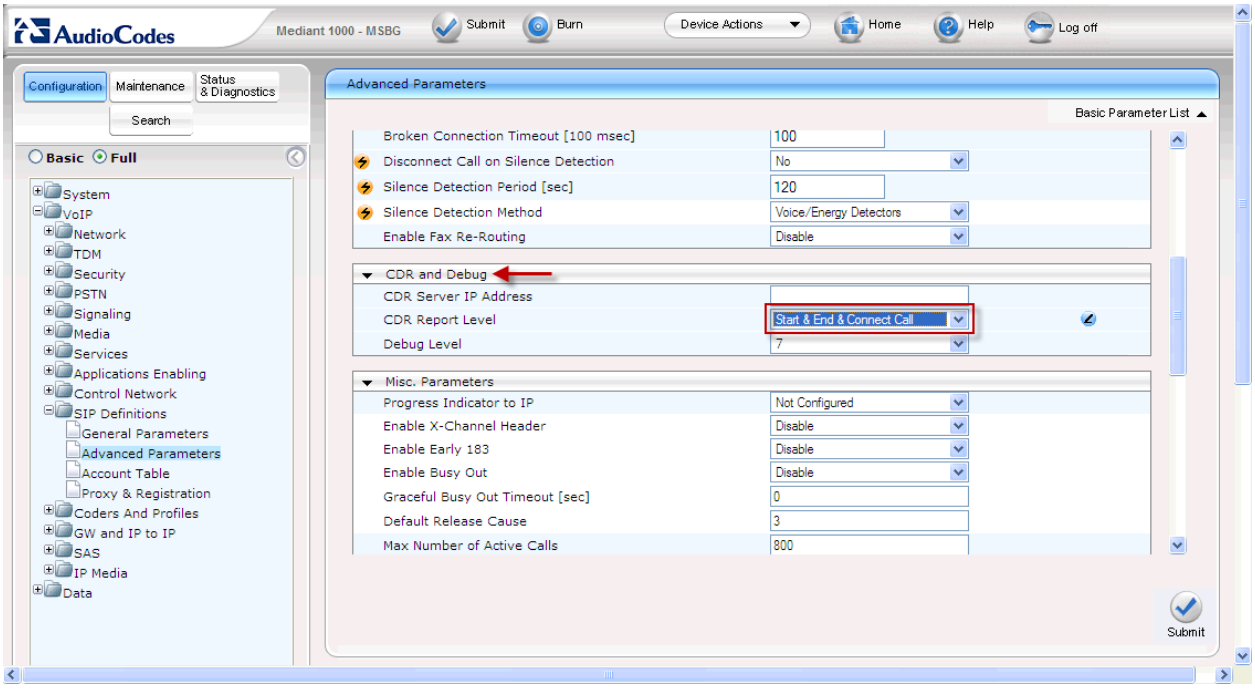



6 Click **Submit.**

## Set CDR Reporting

CDR (Call Data Record) information is helpful when interpreting syslog traces. Here again, we set the option for the most robust reporting.

1. Select the Configuration tab and navigate to VOIP > SIP Definitions > Advanced Parameters.
2. Scroll down to the **CDR and Debug** section.
3. Optionally you may set the CDR Server IP Address. If not set it will log to the syslog server IP address set in the previous step.
4. Set CDR Report Level to **Start & End & Connect Call**.
5. Click **Submit**.

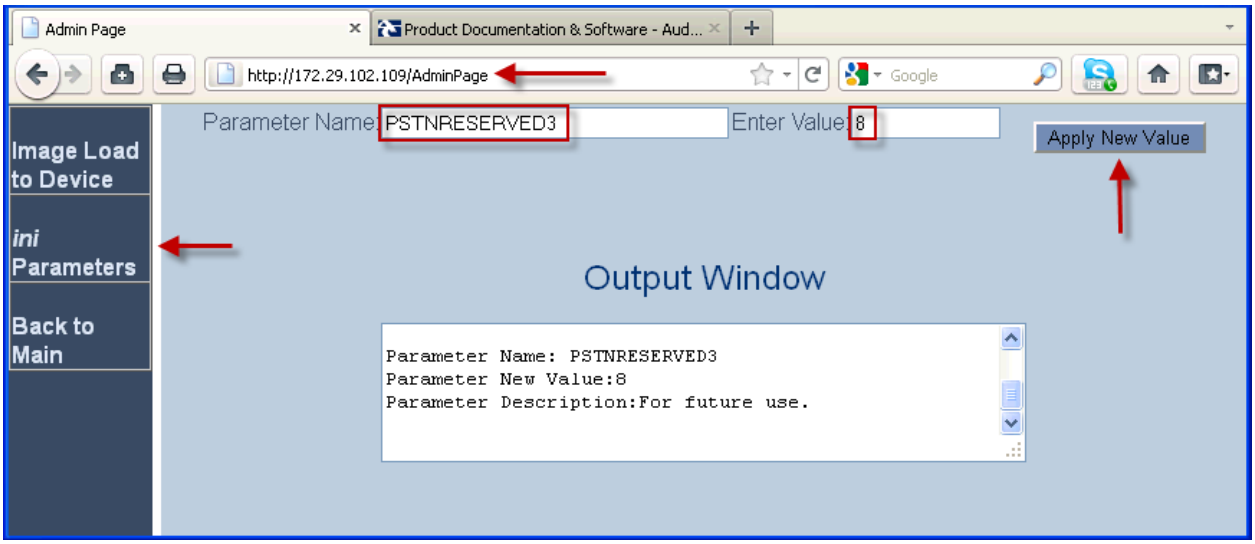


## Configure additional syslog trace settings

Additional trace settings should be set on the Admin Page.

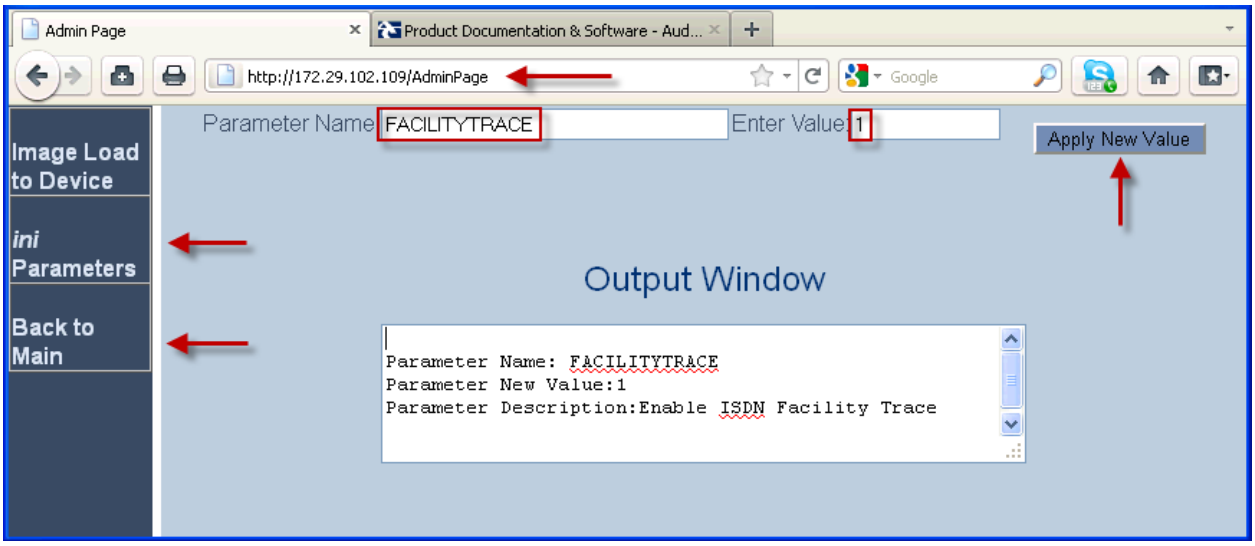
PSTNreserved3: Configures the low level PSTN i.e. Q931 trace messages to be sent to syslog.

1. Enter **AdminPage** after the IP address in the browser as shown in the screen below.
2. Select *ini* Parameters in the Nav pane on the left.
3. Enter **PSTNReserved3** and the value 8
4. Click **Apply New Value**.




Facility Trace: Setting this parameter allows you to display the description of the facility messages in the syslog.

1. Type **FacilityTrace** in the Parameter Name field and **1** in the Enter Value field.
2. Click the **Apply New Value** button.



3 Click **Back to Main** when finished.

# 7. Enable SAS Application

1 Select the Configuration tab and navigate to VOIP > Applications Enabling > Applications Enabling.

2 Using the drop-down for the Enable SAS field, choose **Enable**

**Tip: View the SAS option**

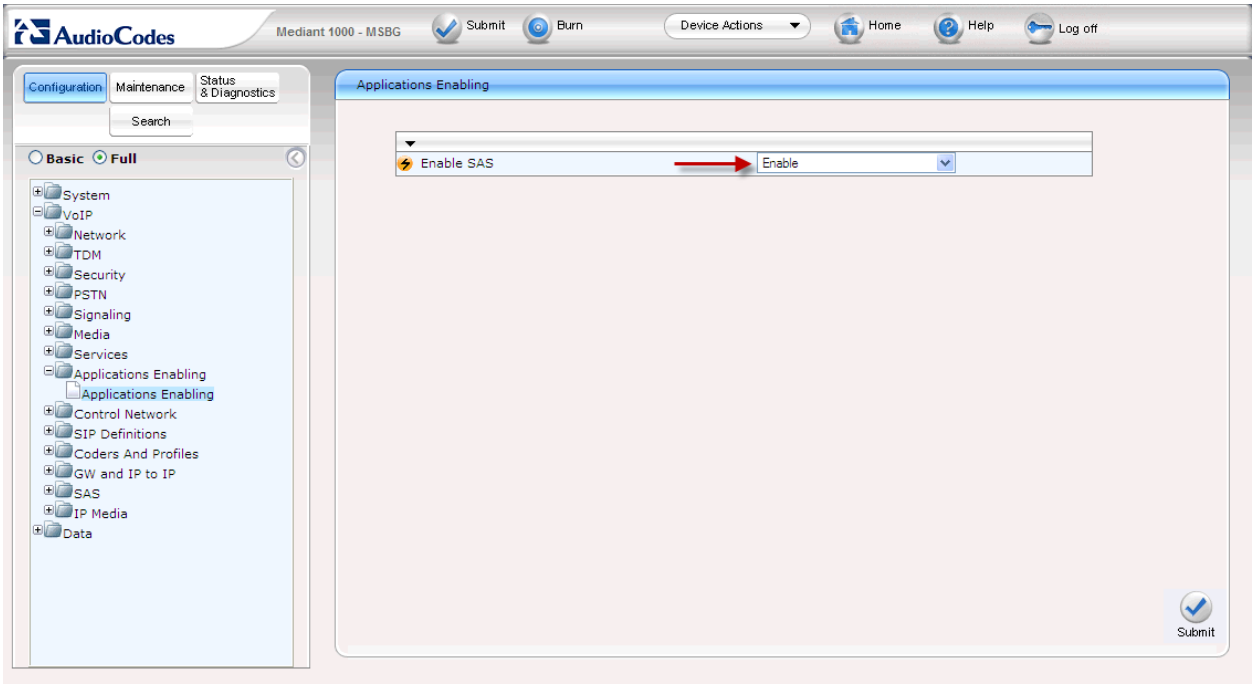
If you do not see the SAS option as the last item on the VOIP menu, ensure you have the Full radio button checked. If it is still not visible, return to the License section and double check to see that SAS is available.

3 Click the **Submit** button.

4 Use Device Actions to reset the Mediant Gateway .

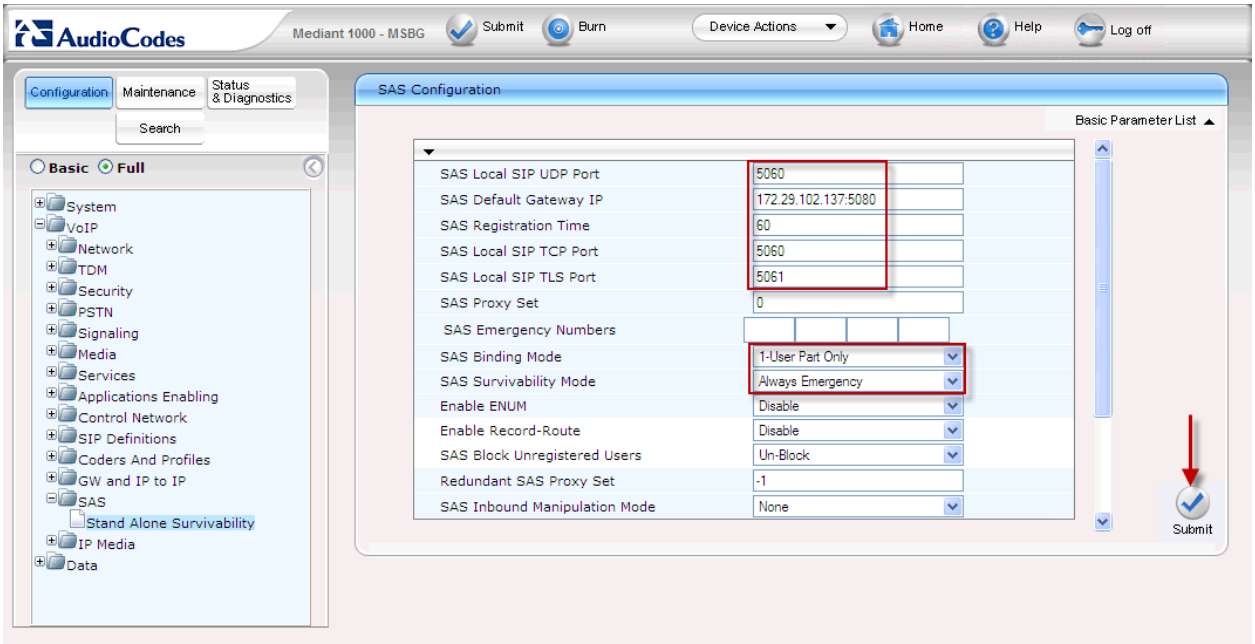
**Tip: The Lightning Bolt Icon**

Any parameter that has the lightning bolt symbol will require a reset in order to take effect.



## Configure SAS

**1** Select the Configuration tab and navigate to VOIP > SAS > Stand Alone Survivability.




**2** Configure these options:

| | |
|---|---|
| SAS Local SIP UDP Port | 5060<br>This allows the SAS application to send and receive SIP signaling on the Mediant Gateway 's port 5060. |
| SAS Default Mediant Gateway IP | The Mediant Gateway application's IP address and port i.e. <ip address>:5080. |
| SAS Registration Time | 60 (seconds)<br>When the phone is powered off or becomes unavailable, this is the amount of time that elapses before the Mediant Gateway will provide a busy alert to caller. See note below. |
| SAS Local SIP TCP Port | 5060 |
| SAS Local SIP TLS Port | 5061 |
| SAS Binding Mode | 1- User Part Only |
| SAS Survivability Mode | Always Emergency |

**3** Click the **Submit** button.

**Caveat: What happens during the timeout?**

Necessarily, we have to set a time period for the Mediant Gateway to realize that the handset is not available. Any timeout creates a window of time where the phone could be turned off or out of range during which calls that come to it will not respond in the usual way. The caller will hear only silence, not a busy tone or a ring. Too short a timeout will over-burden the Mediant Gateway with repeated registration requests. In this document we have recommended a 60 second timeout with the understanding that sometimes the phone will give an unexpected response to a caller.

# 8. Configure Mediant Gateway Application SIP parameters

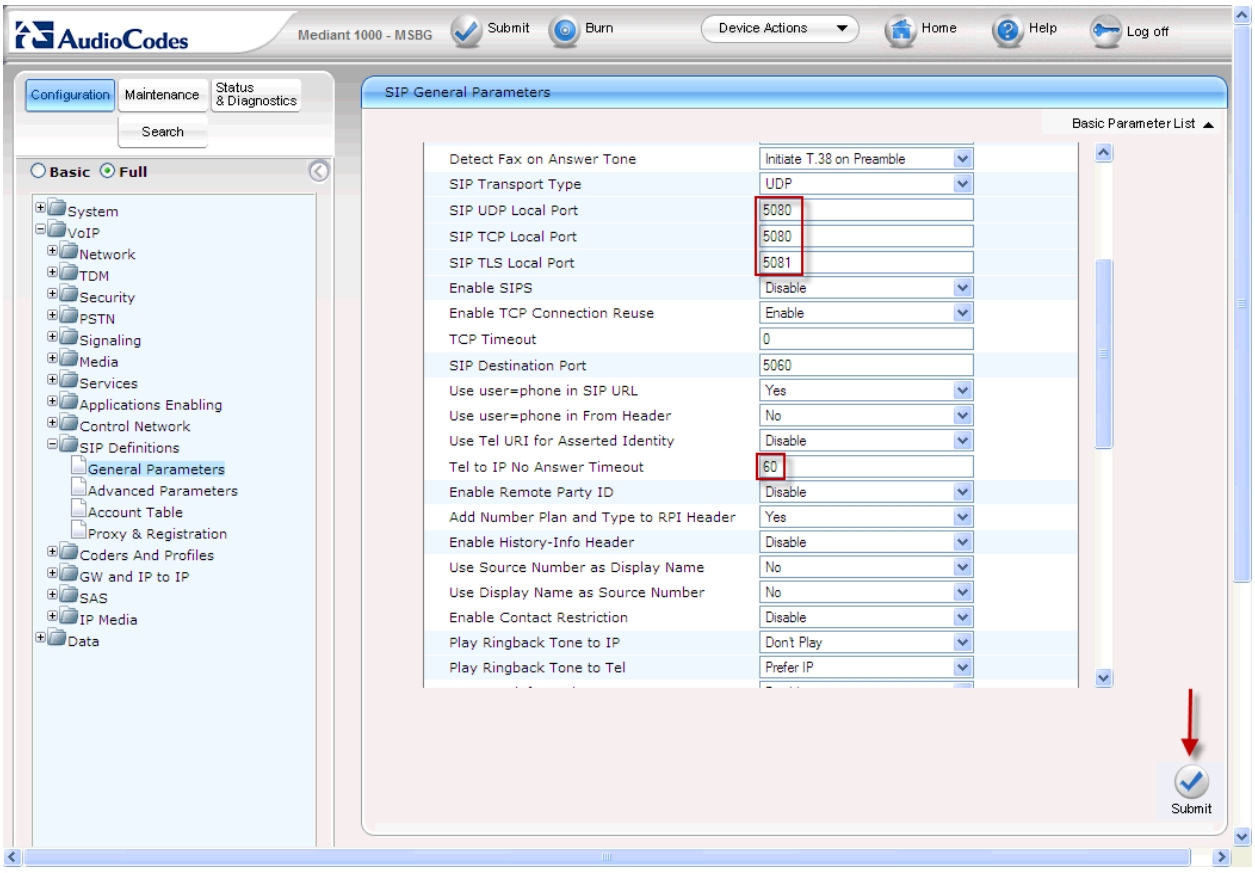
1 Select the Configuration tab and navigate to VOIP > SIP Definitions > General Parameters.

2 Configure these options:

| | |
|---|---|
| SIP UDP Local Port | 5080. |
| SIP TCP Local Port | 5080. |
| SIP TLS Local Port | 5081 |
| Tel to IP No Answer Timeout | Change this value to 60 seconds to match the SAS Registration Time. |

**Note: What happens during the timeout?**

The 60 second timeout creates a window of time where the phone could be turned off or out of range during which calls that come to it will not respond in the usual way. The caller will hear only silence, not a busy tone or a ring.




3 Click the **Submit** button.

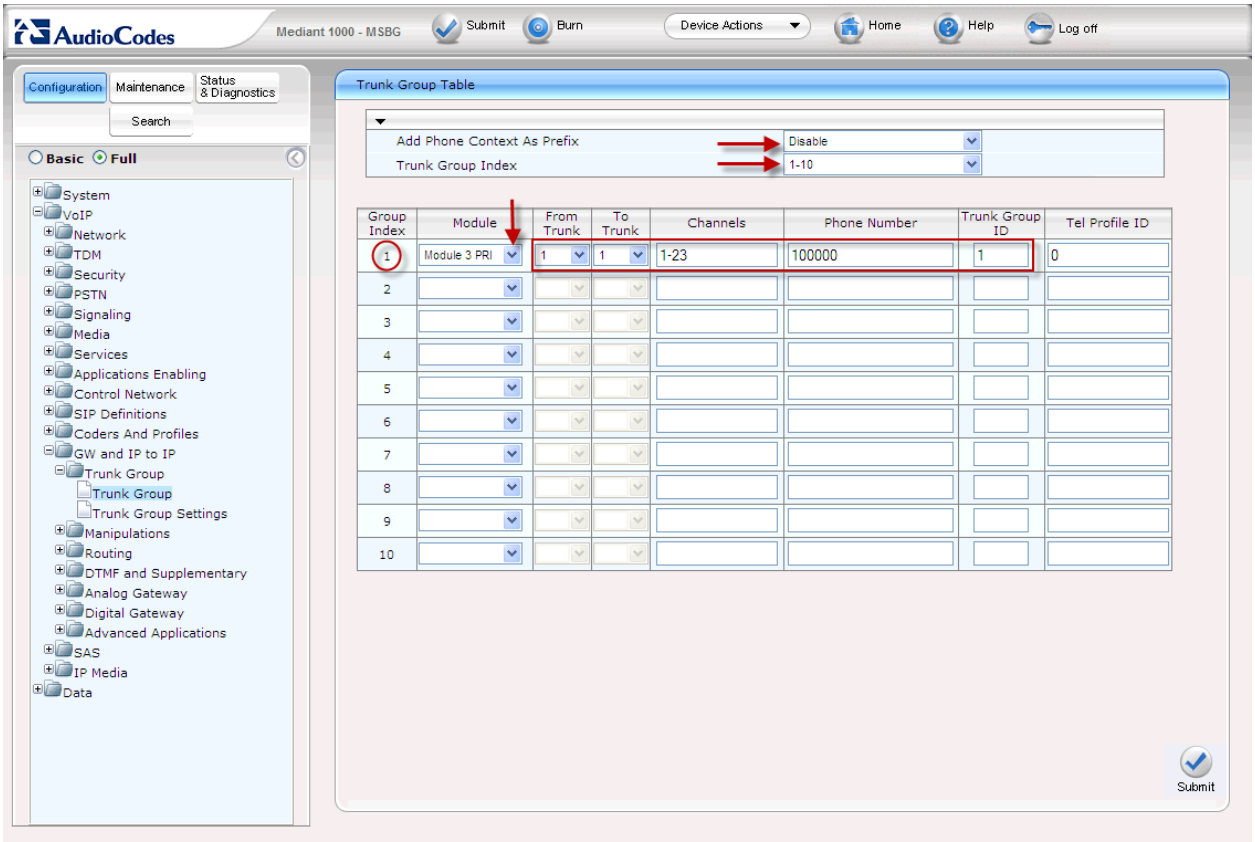
# 9. Configure Mediant Gateway Trunk Group

Trunk group is a local entity that the Mediant Gateway will use for call routing. For most applications all available channels will be aggregated into one trunk group.

**Admin Tip: Adding multiple PRIs to a trunk group?**

If you are configuring multiple PRIs, review Chapter 10 Expanding your System. You will need to go through the configuration sequence below regardless of how many trunks are configured.

1 Select the Configuration tab and navigate to VOIP > GW and IP to IP > Trunk Group > Trunk Group.




2 Add Phone Context as Prefix: Ensure parameter is set to **Disable**.

3 Trunk Group Index: Using the drop-down menu, ensure the parameter is set to **1-10**.

4 For Group Index 1:

| | |
|---|---|
| Module | Use the dropdown list to select the correct module. |
| From Trunk | 1 |
| To Trunk | 1 |
| Channels | 1-23 (1-30 for E1) |
| Phone Number | Enter 100000 (see note below) |
| Trunk Group ID | 1 |

**Tip: Setting a sensible Phone Number**

The Phone Number is the starting point of a range of numbers that the Mediant Gateway uses internally. When choosing a phone number choose a range of numbers that is outside the range of extensions used in your facility. The range will be from the configured phone number to the phone number plus the number of DS0 voice channels, i.e. for a single T1, 23 channels, the Mediant Gateway would use extensions 100000 through 100022. We are using 100000 here as it is unlikely that any facility will have extensions of this length. DO NOT USE EXTENSIONS THAT ARE USED ELSEWHERE IN THE SYSTEM.

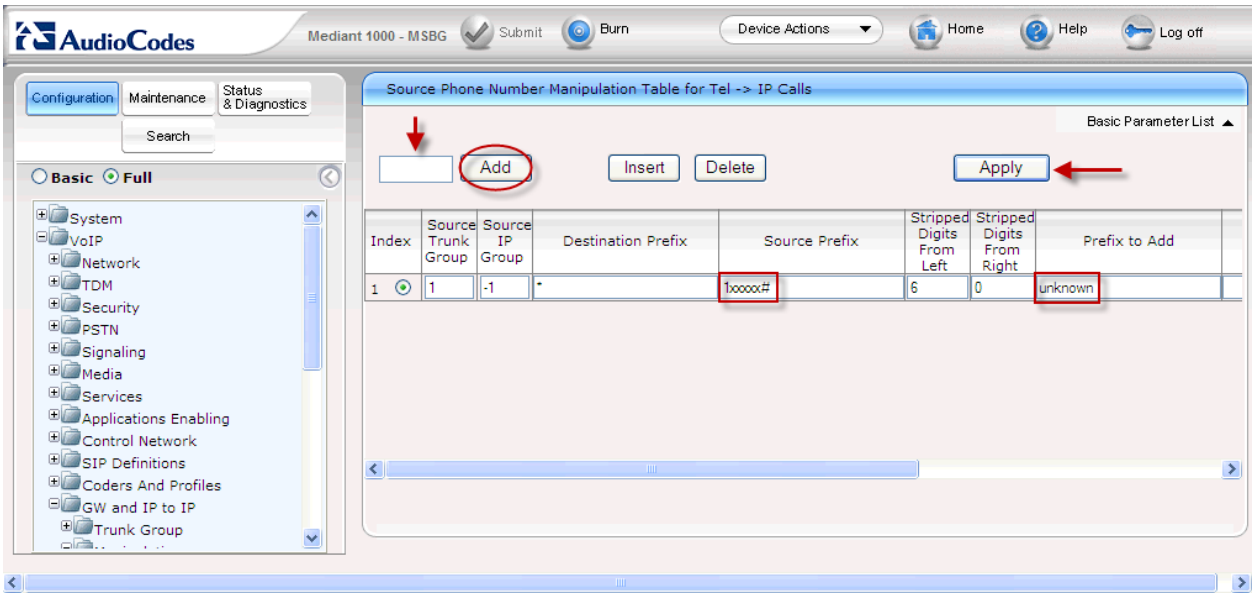
5 Press the **Submit** button.

**To set “unknown” text to display if the Caller ID is not provided.**

1 Select the Configuration tab and navigate to VOIP > GW and IP to IP > Manipulations > Source Number Tel -> IP.

2 Add a source Trunk Group by entering 1 in the field and clicking the Add button. Set or verify the following parameters:

| | |
|---|---|
| Source IP Group | -1 |
| Destination Prefix | * |
| Source Prefix | 1000xx#<br>This number is derived from the Phone Number entered in the Group Index for the Trunk Group configured previously. |
| Stripped Digits from Left | 6 |
| Stripped Digits from Right | 0 |
| Prefix to Add | unknown |
| Suffix to Add | [leave blank] |




**3** Click **Apply**.

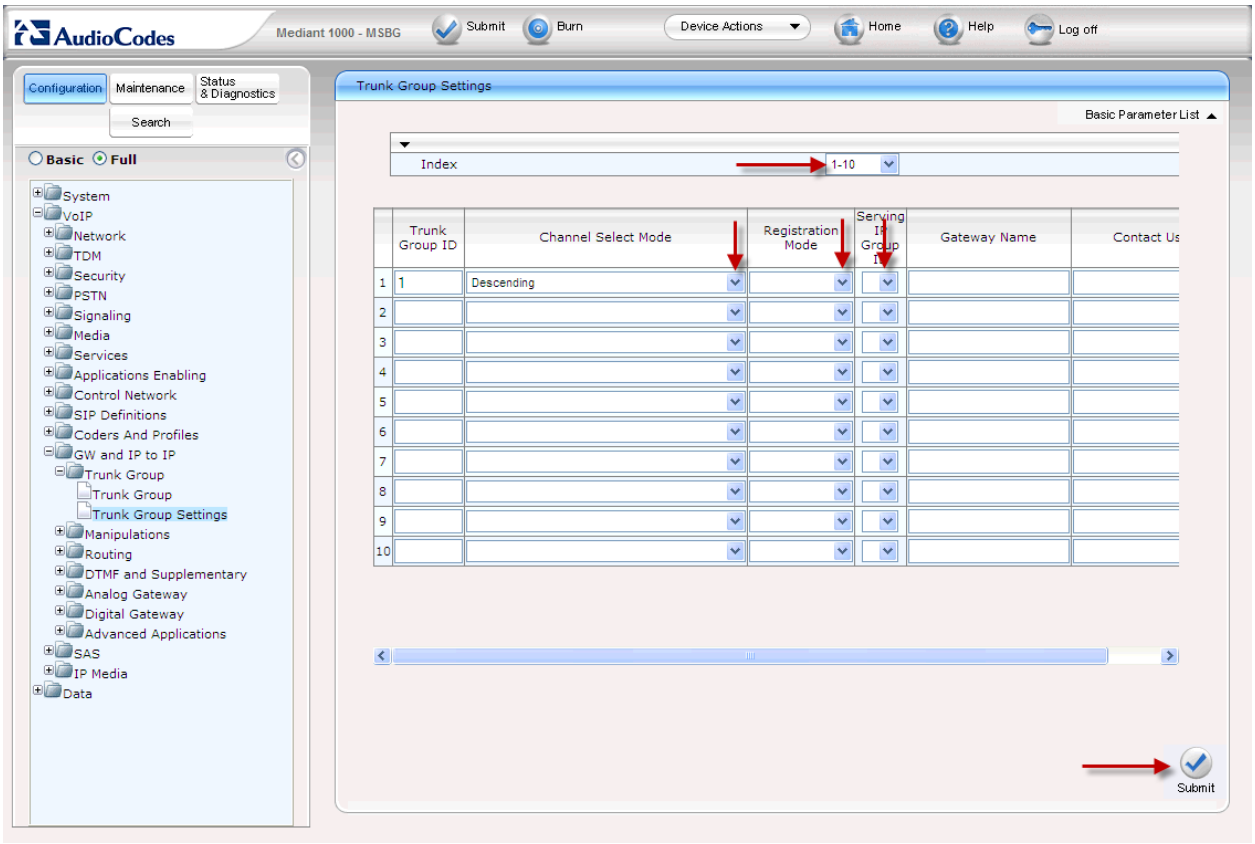
# 10. Configure Mediant Gateway Trunk Group Settings

**1** Select the Configuration tab and navigate to VOIP > GW and IP to IP > Trunk Group > Trunk Group Settings.

**2** Set Index to **1-10** using the dropdown menu.

**3** For row 1:

| | |
|---|---|
| Trunk Group ID | 1 |
| Channel Select Mode | Descending |
| | Descending assumes that the PBX uses ascending mode. Therefore we are setting the opposite channel mode. Double check with the PBX to ensure the opposite setting is used here. Refer to the AudioCodes user manual for explanation about all supported channel select modes. |
| Registration Mode | [blank] |
| Serving IP Group ID | [blank] |



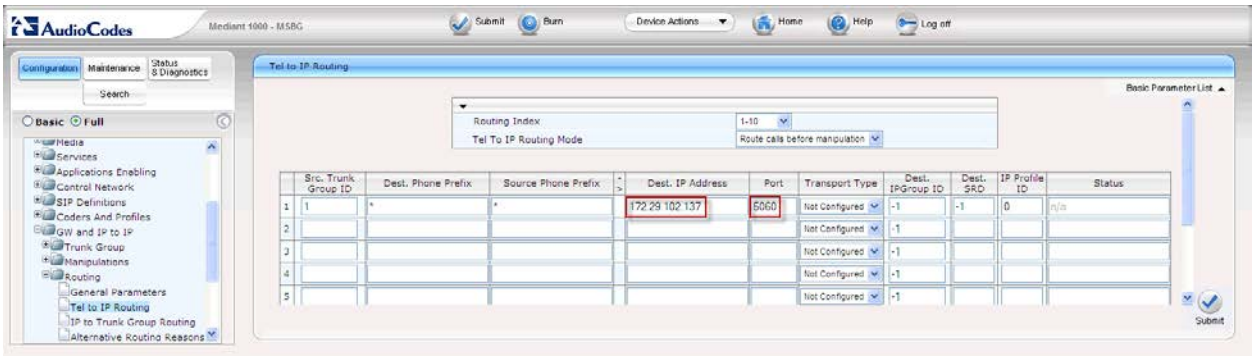

**4** Click **Submit.**

# 11. Configure Tel to IP Routing

Configure Tel to IP Routing is used to set up routing from PRI to the SAS application which manages the IP phone registration.

1. Select the Configuration tab and navigate to VOIP > GW and IP to IP > Routing > Tel to IP Routing.
2. Set Routing Index to **1-10** using the dropdown menu.
3. Set Tel to IP Routing Mode to **Route calls before manipulation.**
4. For Index 1, set or ensure:

| | |
|---|---|
| Source Trunk Group ID | 1 |
| Destination Phone Prefix | * |
| Source Phone Prefix | * |
| Dest IP Address | Mediant Gateway IP Address |
| Port | Set to the configured SAS port, i.e. 5060 |
| Transport Type | Not Configured |
| Dest IP Group ID | -1 |




5. Click **Submit**.

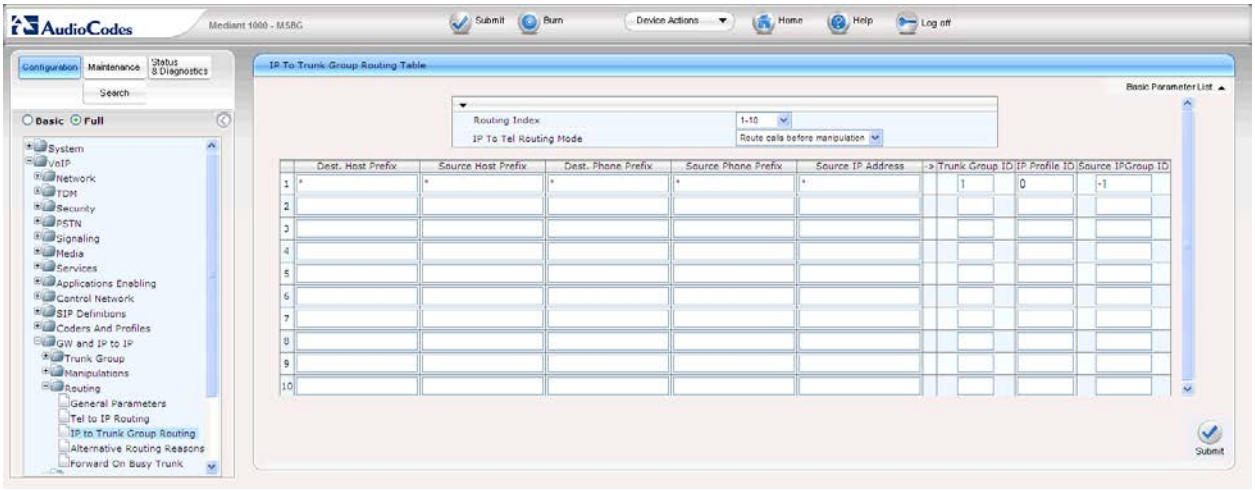
# 12. Configure IP to Trunk Routing

Configure IP to Trunk Routing is used to set up routing from IP telephony to PRI. All calls that would not be routed internally to another SIP registration will be routed to the PBX.

1 Select the Configuration tab and navigate to VOIP > GW and IP to IP > Routing > IP to Trunk Group Routing.

2 Set the following parameters

| | |
|---|---|
| Dest Host Prefix | * |
| Source Host Prefix | * |
| Dest IP Phone Prefix | * |
| Source Phone Prefix | * |
| Source IP Address | * |
| Trunk Group ID | 1 |
| IP Profile ID | 0 |
| Source IP Group ID | -1 |




3 Click **Submit.**

## Avoiding a Routing Loop

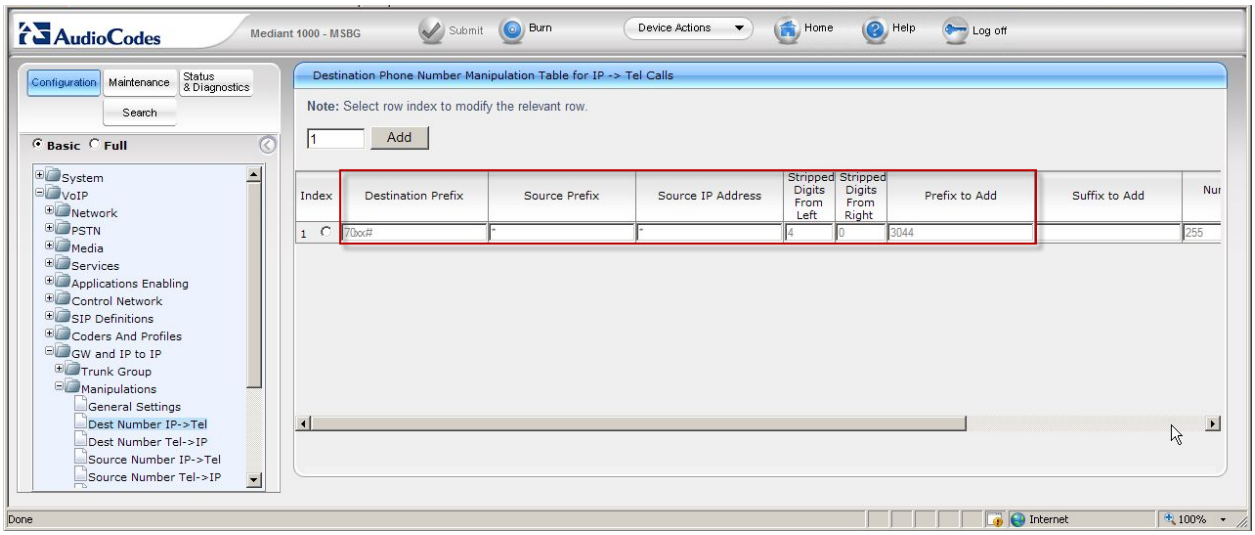
In the last section, we told the Mediant Gateway to route all calls that are not found registered to the SAS to the PRI and on to the PBX. This keeps our routing rules in the Mediant Gateway relatively simple, and allows almost all of our dialplan and routing rules to be maintained on the PBX. However, we must tell the Mediant Gateway what to do if it receives a call from the PBX intended for a station that is not found to be currently registered to the SAS. This could occur if an extension defined on the PBX as part of a block that "belongs" to the Mediant Gateway (see section 6 of Chapter 8) is sent to the Mediant Gateway and is not found to be currently registered, or if that station was simply never built, but happens to reside within the range of extensions defined on the PBX to be sent out to the Mediant Gateway . If we do not perform this step, the Mediant Gateway would send a call to an unregistered station back to the PBX. The PBX would check its rules and send these calls back to the Mediant Gateway . This could go on for some time. In our testing this "routing loop" eventually resolved itself without eating up all of the bearer channels on the PRI, and the calling party was presented with a re-order tone. However, we can make more efficient use of our resources and provide callers with a better indicator of what has happened.

Options for handling such calls could include routing them to a vacant extension to a recorded announcement back on the PBX telling callers that they have dialed a number that is currently unavailable. Or you could have them ring to a desk station somewhere. Alternatively you could route them to a non-existent number on the PBX and callers would simply be given a re-order tone.

1. Navigate to VOIP->GW and IP to IP->Manipulations -> Dest Number IP->Tel
2. Add a Destination Index for each unique block of extensions you have defined on the Mediant Gateway (in our example we have only one: 70xx).
3. Configure:

| | |
|---|---|
| Destination Prefix | This is the block of numbers you are sending to the Mediant Gateway followed by a # sign. Note that the Mediant Gateway will not look at this table to route these calls unless it has already checked the SAS proxy and determined that the phone is currently unregistered. (In our example we used 70xx#) |
| Source Prefix | * |
| Source IP Address | * |
| Stripped Digits From Left | Enter the extension's length. (We stripped all four digits in our example) |
| Stripped Digits From Right | 0 |
| Prefix to Add | Enter the extension number you wish the call to re-route to: For our testing purposes we pointed them to a CCMS station (x-3044) residing on the PBX. |

4. The remaining fields should stay at the default value.




5 **Submit** and **Burn**.

**Note: Ensure correspondence between PBX and Mediant Gateway**

Configure a destination index for every unique set of numbers that you define in the AAR routing table (see Chapter 6 section 7). Using this method you will have a one to one correspondence between patterns entered into the AAR table destined for this Mediant Gateway and pattern indices you create here.

## Detecting a routing loop

Routing loops are detected by the appearance of certain patters in the syslog. By way of explanation, consider the following example.

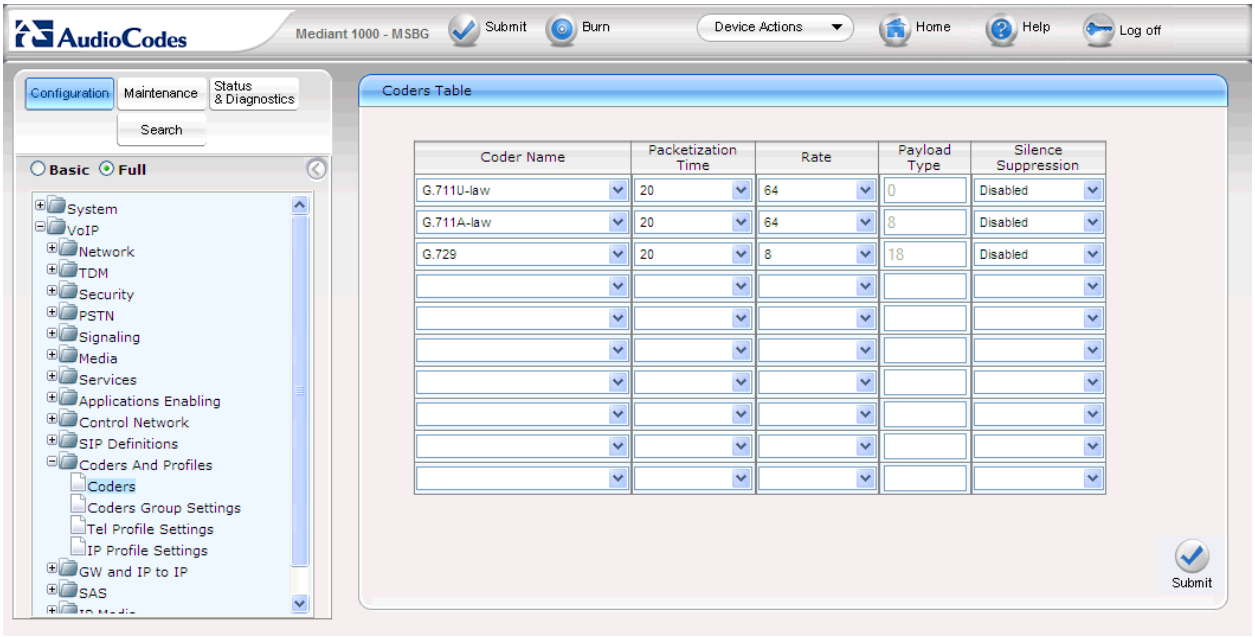
Using our example number ranges we will define extensions 7xxx to reside on the Mediant Gateway, and tell the PBX to send all calls destined for extensions in the 7xxx range out the PRI circuit to the Mediant Gateway. Imagine if extension 7001 was not currently registered on the Gateway. Without providing an alternate number to route such calls to, the Mediant Gateway would just send the request back to the PBX. The PBX would look at the invite and route the call back to the Mediant Gateway. This is a loop. Here we have the D-channel attempting to set up this call, but since no one is around to accept it, the call would never get set up. It would be rather difficult to tell this was occurring without looking at syslog output from the Mediant Gateway. In our testing our syslogs showed many repeated attempts to set up calls to the same number going back and forth between the Mediant Gateway and the PBX. The above configuration would resolve this.

# 13. Configure Default Coder Group

1 Select the Configuration tab and navigate to VOIP > Coders and Profiles > Coders.

2 Using the drop-down, set the Coder Name to G.711U-law, G.711A law and G729 as shown below.

3 Set Silence Suppression to Disabled




4 Click **Submit**.

**Admin Tip: G.722 restriction**

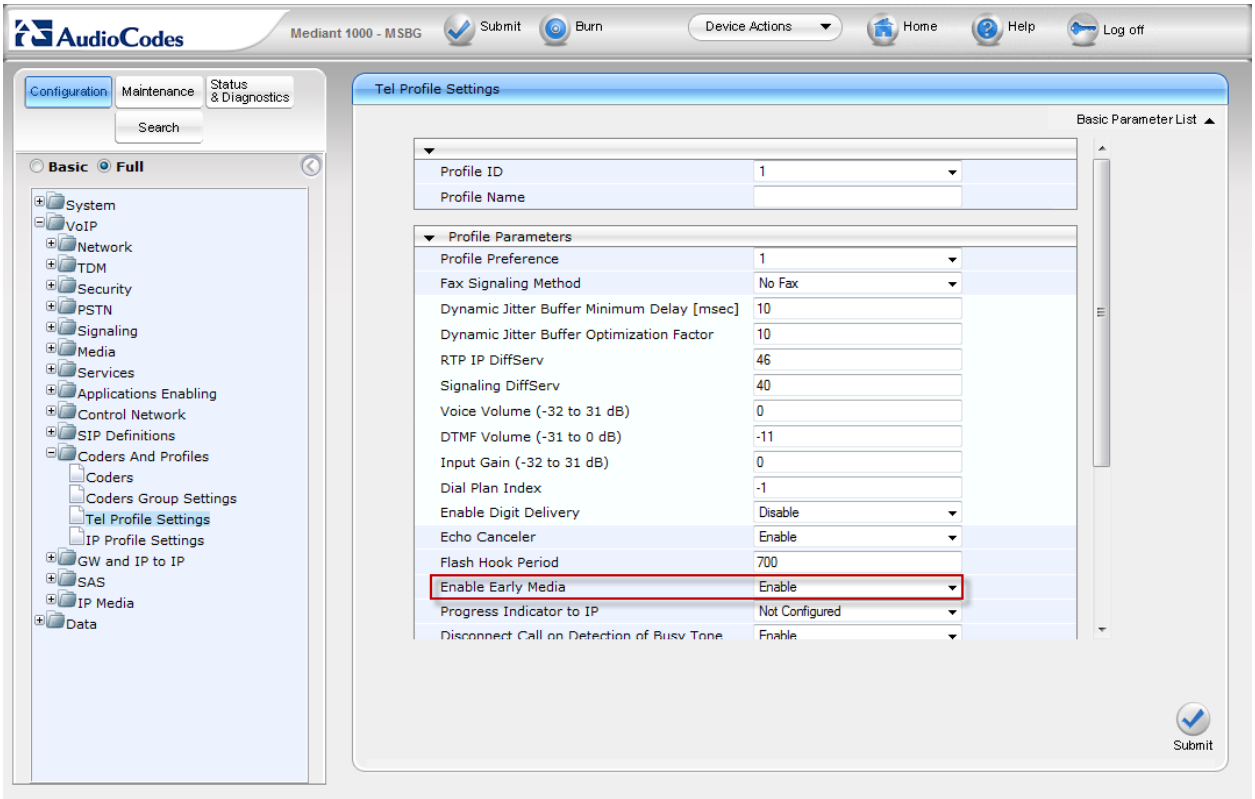
G.722 (High Definition audio) will only work on intra-Mediant Gateway calls.

# 14. Enable Early Media

To prevent “clipping” of audio when first connecting an IP call, Early Media should be enabled. You might notice this type of clipping when first connecting to an IVR or Voicemail system if this parameter is not enabled.

1 Select the Configuration tab and navigate to VOIP > Coders and Profiles > Tel Profile Settings.

2 Set **Enable Early Media** to **Enable**.



# 15. TDM configuration

TDM Bus settings is used to configure the signal encoding used between the Mediant Gateway and the PBX.

1 Select the Configuration tab and navigate to VOIP > TDM > TDM Bus Settings.

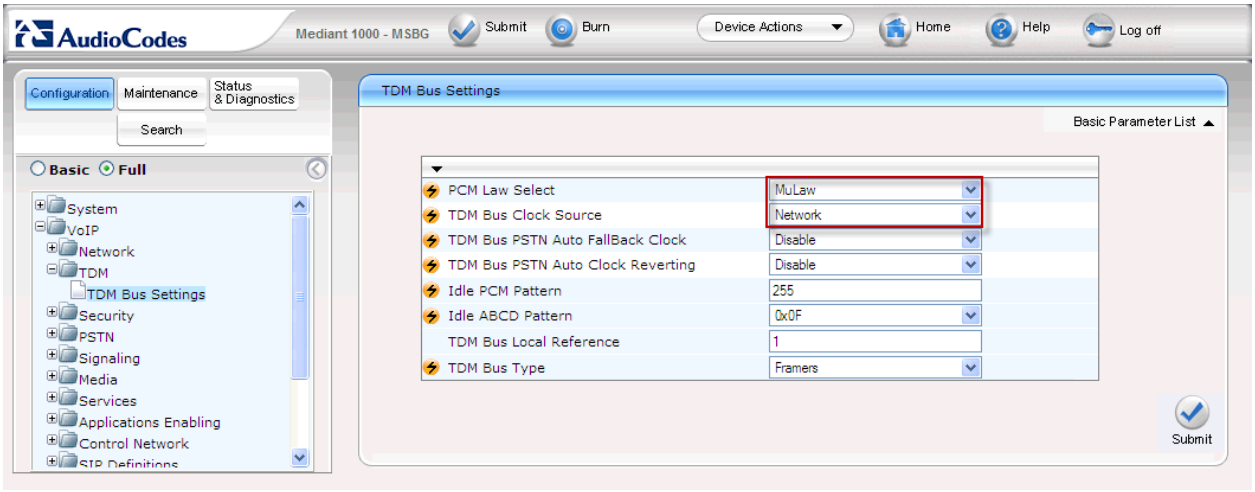
2 If your physical channel is T1 set PCM Law Select to **MuLaw**. For E1 set **ALaw**. Note that there are very rare exceptions but this setting must match the configuration you create on the PBX side.

3 Set TDM Bus Clock Source to **Network**

**Note: Multiple Trunks**

If you have multiple trunks please see Chapter 10: Expanding your System.

4 Click **Submit**.

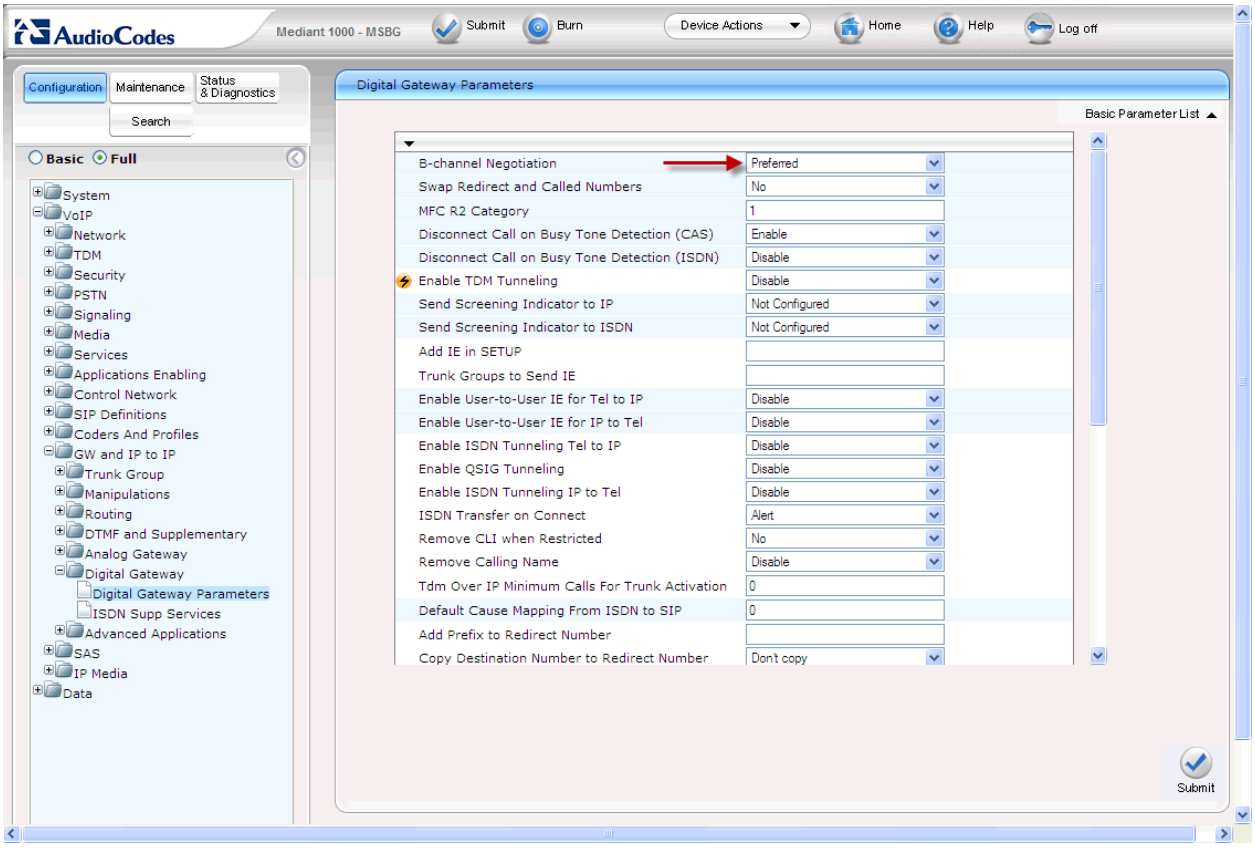


# 16. B-Channel negotiation

Configures the most flexible behavior for the B-channel negotiation.

1 Select the Configuration tab and navigate to VOIP > GW and IP to IP > Digital Gateway > Digital Gateway Parameters.

2 Set B-channel negotiation to **Preferred**.




3 Click **Submit**.

# 17. Setting up the PRI

The parameters you set in the Mediant Gateway will depend on your PBX's PRI settings, but these can be used as a reference

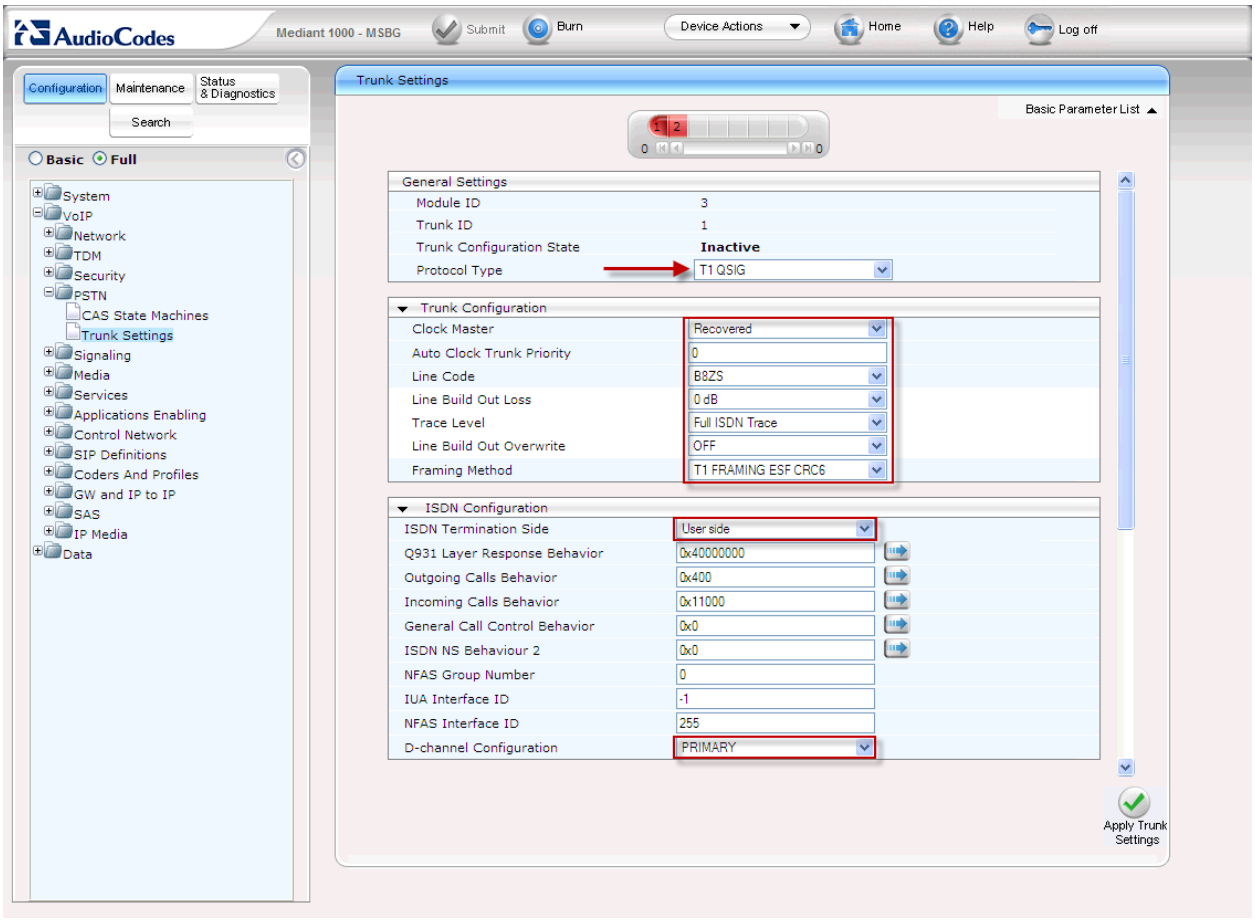
1. Select the Configuration tab and navigate to VOIP > PSTN > Trunk Settings.
2. In the Protocol Type field, select **T1 Q.SIG**.

**Admin Tip: If the trunk is already started…**

If the trunk is already started, you will not be able to edit trunk parameters unless you shut down the trunk. If this is the case, click the **Stop Trunk** button.

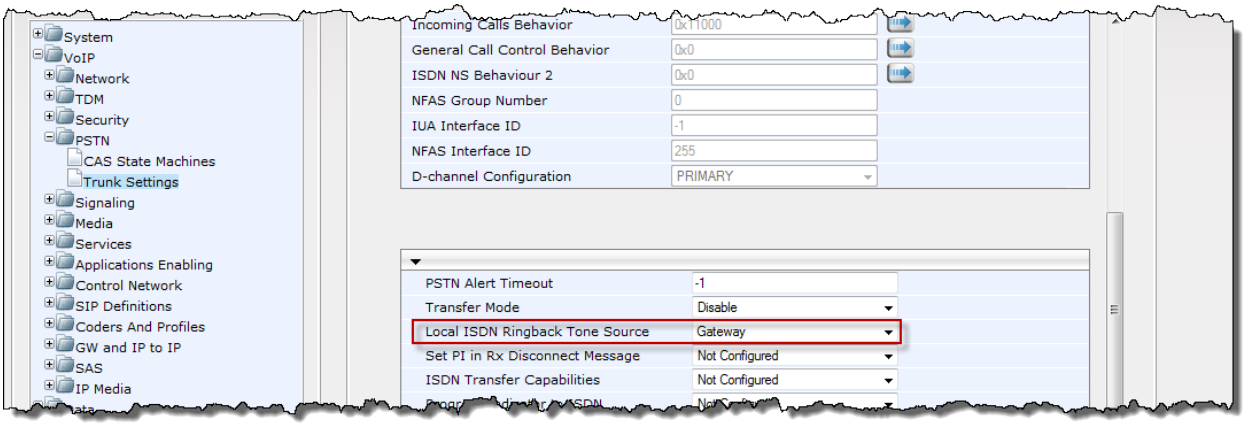
3. When you first set up the Mediant Gateway or change the Protocol type field, click the Apply Trunk Settings and Burn.
4. Verify the following settings:

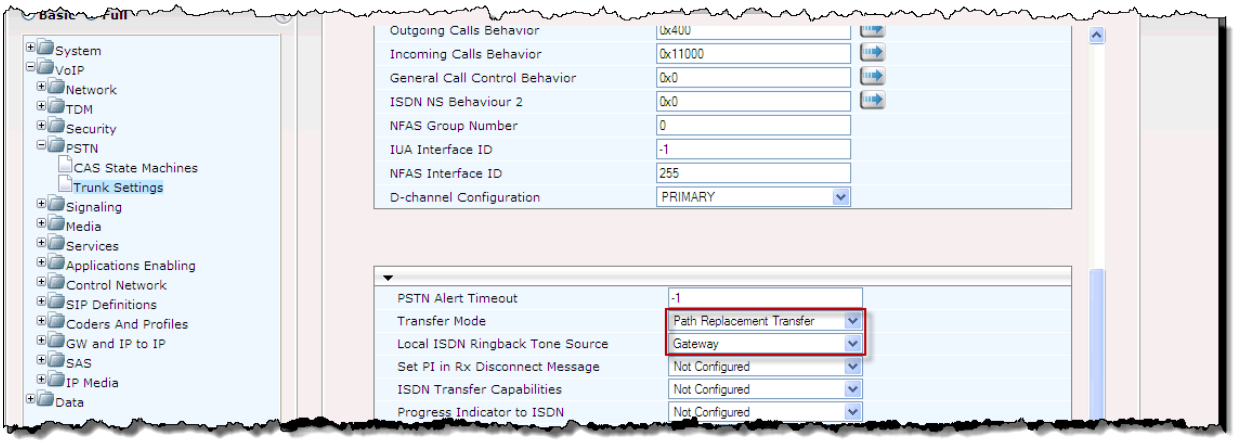
| | |
|---|---|
| Clock Master | Recovered (this means that the Mediant Gateway will recover the clock from the T1 signal instead of using the Mediant Gateway internal clock) |
| Auto Clock Trunk Priority | leave at default 0 |
| Line Code | B8ZS |
| Line Build Out Loss | 0 dB |
| Trace Level | Full ISDN Trace to produce all messages in syslog |
| Line Build Out Overwrite | OFF |
| Framing Method | T1 FRAMING ESF CRC6 (important to verify that this setting matches the PBX. In many cases the PBX may not use CRC6 in which case select the appropriate variant from the dropdown menu) |
| ISDN Termination Side | User Side |
| D-channel configuration | PRIMARY |




scroll to:

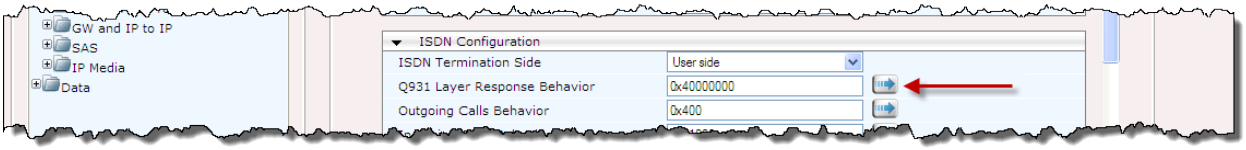
**a** Local ISDN Ringback Tone Source and set it to **Gateway.**



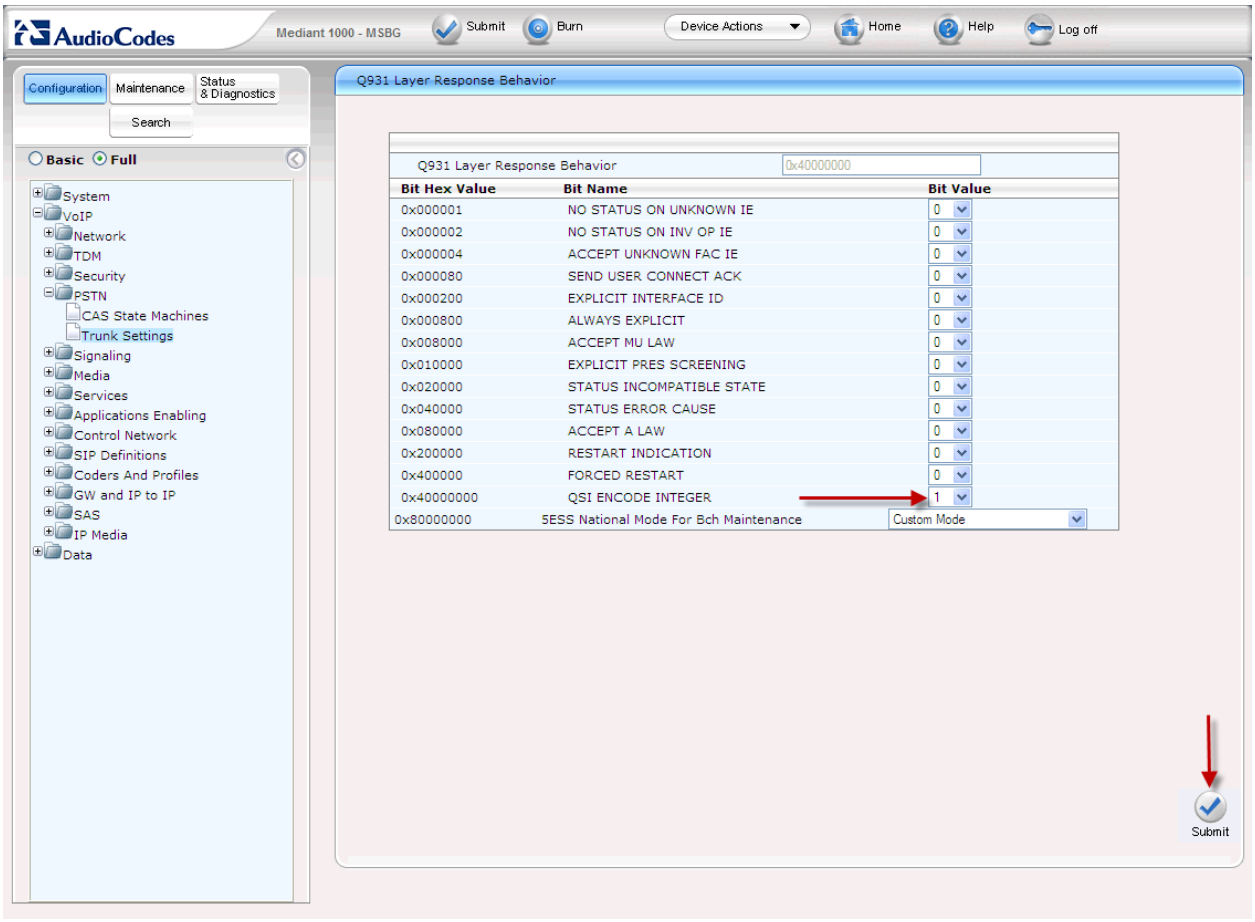



**b** Click **Apply Trunk Settings**.

## Q931 Layer Response Behavior



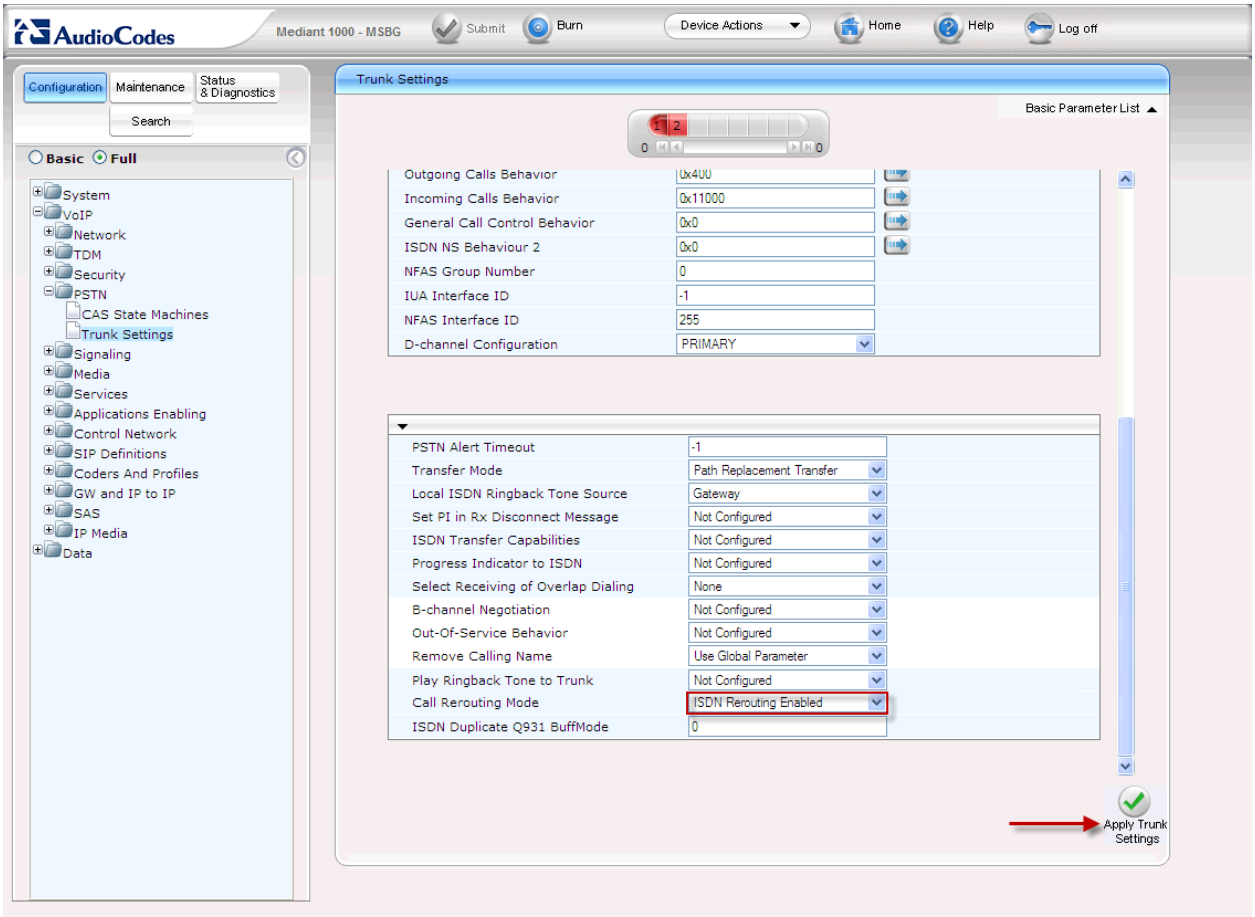

1. Scroll up to the Q931 Layer Response Behavior option and click the arrow to the right of the Q931 Layer Response Behavior row.
2. Set **QSI ENCODE INTEGER** to **1**. This is the usual setting for an Avaya and other PBX. If left at 0 the Mediant Gateway will use ASN.1 encoding.
3. Click **Submit**.




### Set Call Rerouting

The call rerouting option enables path replacement by the PBX instead of by the SIP side during call forward.

1. Select the Configuration tab and navigate to VOIP > PSTN > Trunk Settings.
2. Scroll to the Call Rerouting Mode field, select **ISDN Rerouting Enabled**




3 After setting the parameters, click the **Apply Trunk Settings** button.

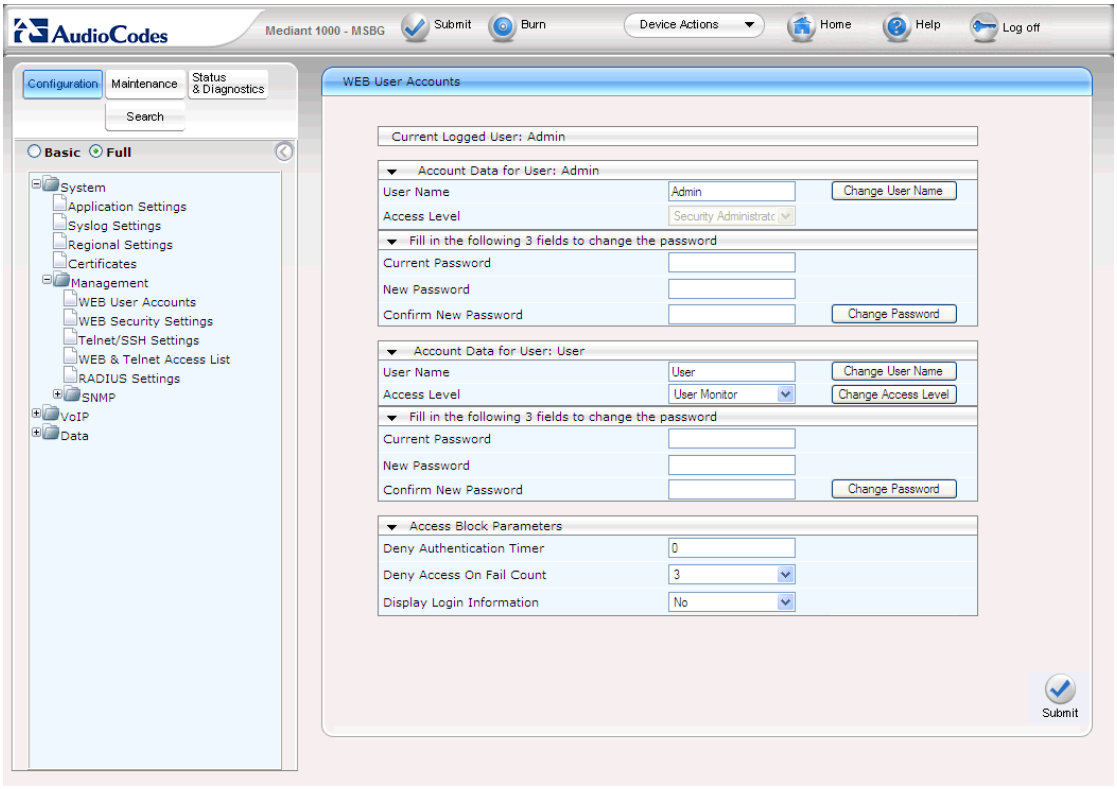
4 Use Device Actions to reset the Mediant Gateway

# 18. Changing the Password

Please secure your system by changing the login username and password.

1 Select the Configuration tab and navigate to System > Management > Web User Accounts.

2 Create an Admin account for each user who will need access to the Mediant Gateway .

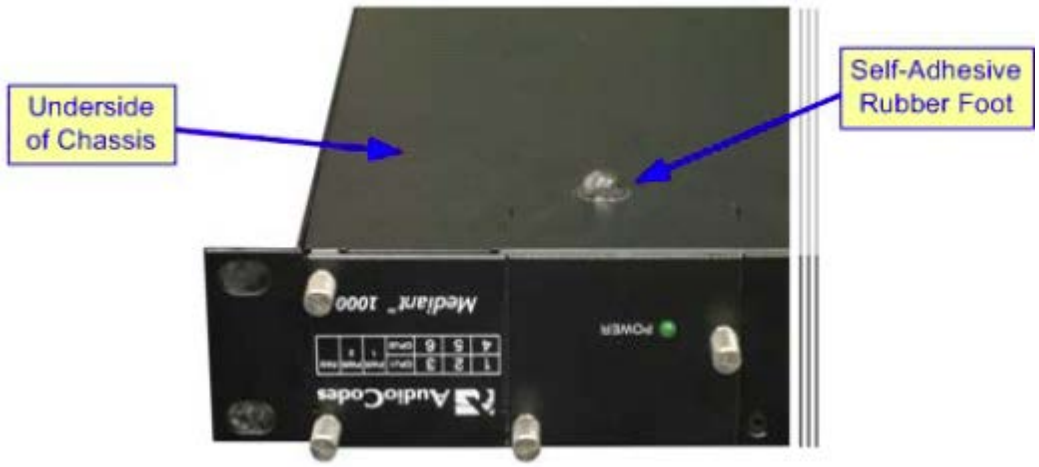


# Chapter 7: Installing the Mediant Gateway

## *Mount the Mediant Gateway*

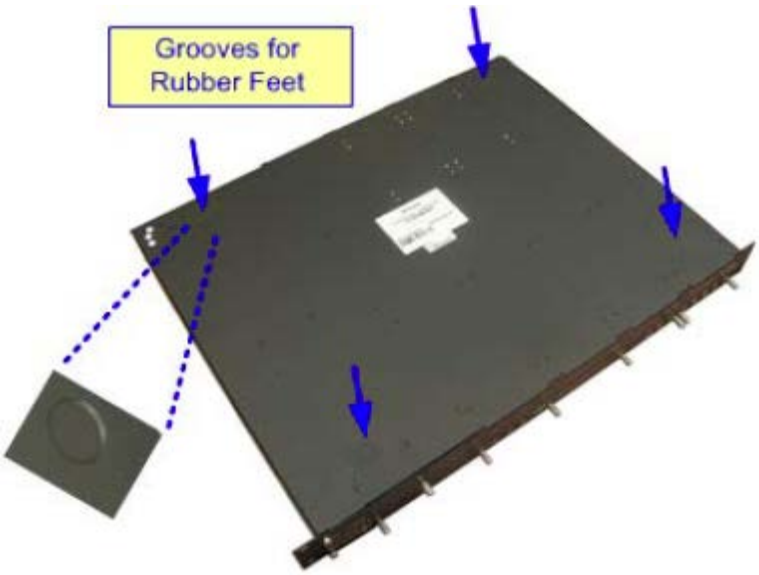
### Desktop mounting

The device can be mounted on a desktop by attaching the four anti-slide bumpers (supplied) to the underside of the device. Once you have attached these bumpers, simply place it on a desktop in the desired position.




**To attach the anti-slide rubber bumpers to the device:**

1. Turn the Mediant Gateway over so that its underside faces up.
2. Locate the four anti-slide grooves on the underside -- one on each of the four corners.




3 Peel each anti-slide rubber foot off the adhesive backing and stick one in each anti-slide groove.

4 Turn the device over so that it rests on its underside and place it in the required position on a desktop.

### 19-inch Rack Mounting

You can install the Mediant Gateway in a standard 19-inch rack that has pre-installed shelves (recommended) or by attaching it directly to the rack frame using the front mounting brackets and user-adapted rear mounting brackets (not supplied).

**Warning: Rack Mount Safety Instructions**

When installing the chassis in a rack, implement the following safety instructions:

- Elevated Operating Temperature: If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient temperature. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (Tma) of 40°C (104°F).
- Reduced Air Flow: Installation of the equipment in a rack should be such that the amount of air flow required for safe operation on the equipment is not compromised. Airflow is side to side so ensure sides are clear.
- Mechanical Loading: Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.
- Circuit Overloading: Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.
- Reliable Grounding: Reliable grounding of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g., use of power strips.)

**To mount the device on a pre-installed shelf in the rack:**

- Place the device on a pre-installed shelf in the rack. We recommend attaching the device's integral front mounting brackets to the rack's frame to prevent it from sliding off the shelf during cabling. Use standard 19-inch rack bolts (not provided) to fasten the front of the device to the frame of the rack.

**To install the device in a rack without shelves:**

1. Position the device in a 19-inch rack and align the front and rear (refer to note below) bracket holes to the holes (of your choosing) in the vertical tracks of the 19-inch rack.
2. Use standard 19-inch rack bolts (not provided) to fasten the brackets to the frame of the rack.

**Caution: Assembling rear brackets**

If you are assembling the rear brackets, please note the following:

- The distance between the screws on each bracket is 28 mm (1.1 inches).
- To attach the brackets, use 4-40 screws with a maximal box penetration length of 3.5 mm (0.14 inch).

# Cabling the Mediant 1000

**Note: Ethernet Cable Type**

Any type of Ethernet cable can be used, not necessarily cross connect, because gigabit connect detects cable type and adjusts settings accordingly. Older systems may require cross cable.

## Connecting to Ground

The device must be permanently connected to ground, using an equipment-grounding conductor.

**Caution: Protective Grounding**

The equipment is classified as Class I EN60950 and UL60950 and must be grounded at all times.

**To ground the device:**

1. Connect an electrically grounded strap of 16 AWG wire (minimum) to the chassis' grounding screw (located on the rear panel), using the supplied washer.
2. Connect the other end of the strap to a protective grounding. This should be in accordance with the regulations enforced in the country of installation.

## Connecting to the LAN

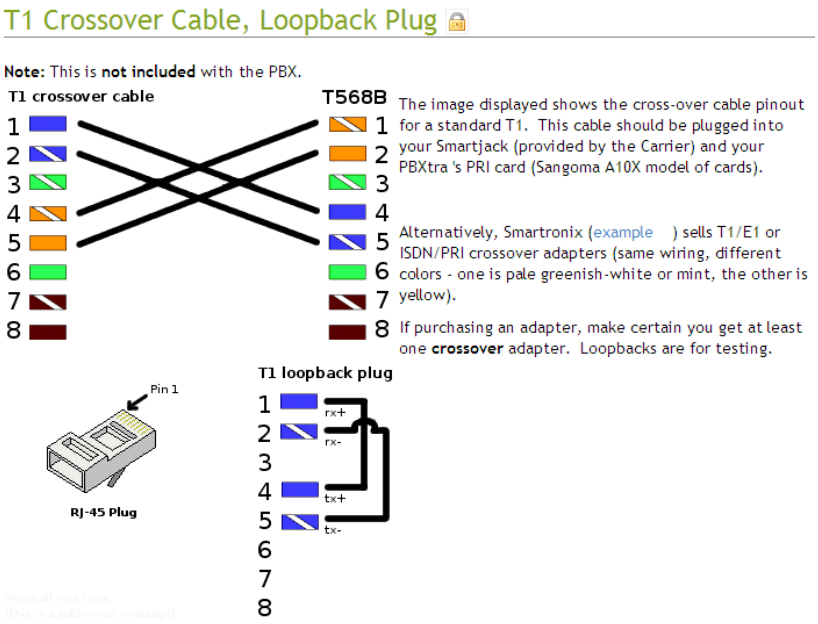
The CRMX module provides three 10/100/1000Base-T Gigabit Ethernet RJ-45 ports for connection to the LAN.

**To connect the device to the LAN using the GbE port:**

1. Attach one end of a straight-through RJ-45 Ethernet Cat 6 or Cat 5e (two-pair Category 5 UTP) cable to any of the module's LAN ports.
2. Attach the other end of the cable directly to the LAN network (e.g., to a Ethernet switch or computer).

## Connecting to E1/T1 Trunks

The procedure below describes the cabling of the device's TRUNKS module interfaces (i.e., E1/T1 trunks). Use a T1 crossover cable.


T1 Crossover Cable, Loopback Plug
Note: This is not included with the PBX.
T1 crossover cable
T568B
1 1
2 2
3 3
4 4
5 5
6 6
7 7
8 8
The image displayed shows the cross-over cable pinout for a standard T1. This cable should be plugged into your Smartjack (provided by the Carrier) and your PBXtra 's PRI card (Sangoma A10X model of cards).
Alternatively, Smartronix (example ) sells T1/E1 or ISDN/PRI crossover adapters (same wiring, different colors - one is pale greenish-white or mint, the other is yellow).
If purchasing an adapter, make certain you get at least one crossover adapter. Loopbacks are for testing.
Pin 1
RJ-45 Plug
T1 loopback plug
1 rx+
2 rx-
3
4 tx+
5 tx-
6
7
8

**Warning: Protection against electrical shock**

To protect against electrical shock and fire, use a 26 AWG min wire to connect T1 or E1 ports to the PSTN.

**To connect the digital trunk interfaces:**

1. Connect the E1/T1 trunk cables to the ports on the device's TRUNKS module(s).
2. Connect the other ends of the trunk cables to your PBX/PSTN switch.

## Connecting to Power

The device can house up to two extractable power supply modules (Power 1 and Power 2), each providing an AC power connector on the device's rear panel. The dual power option provides the device with power redundancy.

**Warning: Protection against electrical shock**

- Units must be connected (by service personnel) to a socket-outlet with a protective grounding connection.
- Use only the AC power cord supplied with the device.

**Note: Using both power units**

- If both power units are used (for load sharing - failure protection / redundancy), ensure that you connect each power supply unit to a different AC supply circuit.
- The two AC power sources must have the same ground potential.

**Connect the device to the power supply:**

On the device's rear panel, connect the left (active) 100-240V~50-60 Hz power socket to a standard electrical outlet using the supplied AC power cord.

The front panel of the power supply module provides a LED (labeled **POWER**) that is lit green when the device is powered up. If this LED is off, a power supply problem may be present.

| Color | State | Description |
|---|---|---|
| Green | On | The LED of each AC power supply is lit green when the power supply is operating correctly. |
| - | Off | Failure / disruption in the AC supply, or the power is currently not being supplied to the device through the AC power supply entry. |

# Chapter 8: Test Basic Functionality

Once the Mediant Gateway configuration is complete, conduct a test of basic handset functionality following the following table. These tests exercise the handsets connectivity with the Mediant Gateway without using the PBX link.

| | |
|---|---|
| Registration | After powering on the phone, check the Mediant Gateway 's AoR screen and check the handset's line registration status. |
| Outgoing Call | Dial another 84-Series handset or SIP endpoint registered with the Mediant Gateway . Verify that a call path is established. The test does not require the PRI link. |
| Incoming Call | Have another registered SIP endpoint call a registered 84-Series handset, ensure the handset rings and a call path is established. The test does not require the PRI link. |
| SIP URL Call | Call an 84-Series handset directly uses the IP address. This bypasses the Mediant Gateway . If this call fails there may be basic network issues. |
| Up to 6 call appearances per line | Each line registration supports by default 24 calls per line. This may be changed using the configuration parameter. |
| Call Hold & Resume | When in call use the hold feature to hold the active call. Retrieve the call using the resume button. |
| Speaker & Mute | When in call try the handset mute and speakerphone capability. |
| Do Not Disturb (DND) | Using the handset set the DND capability, and try calling the handset, it should not ring, and the calling party should receive an busy tone. |
| Transfer (Attended/ Unattended) | If three wireless handsets are available, set up a call between two handsets, then using the phone softkey redirect the call to the third handset using blind or attended transfer. Verify the call is handed off to the third handset. |

# Chapter 9: Configuration Requirements of the Avaya Communication Manager

This configuration assumes that the Avaya Communication Manager is already installed in the facility and has at least one available PRI card.

**Admin Tip: Avaya Communication Manager software version supported.**

The configuration referenced below was obtained from an Avaya Communications Manager running version 5.2. Supported versions range from 5.0 to 6.1. The screens and parameters referenced should be similar on these versions as well.

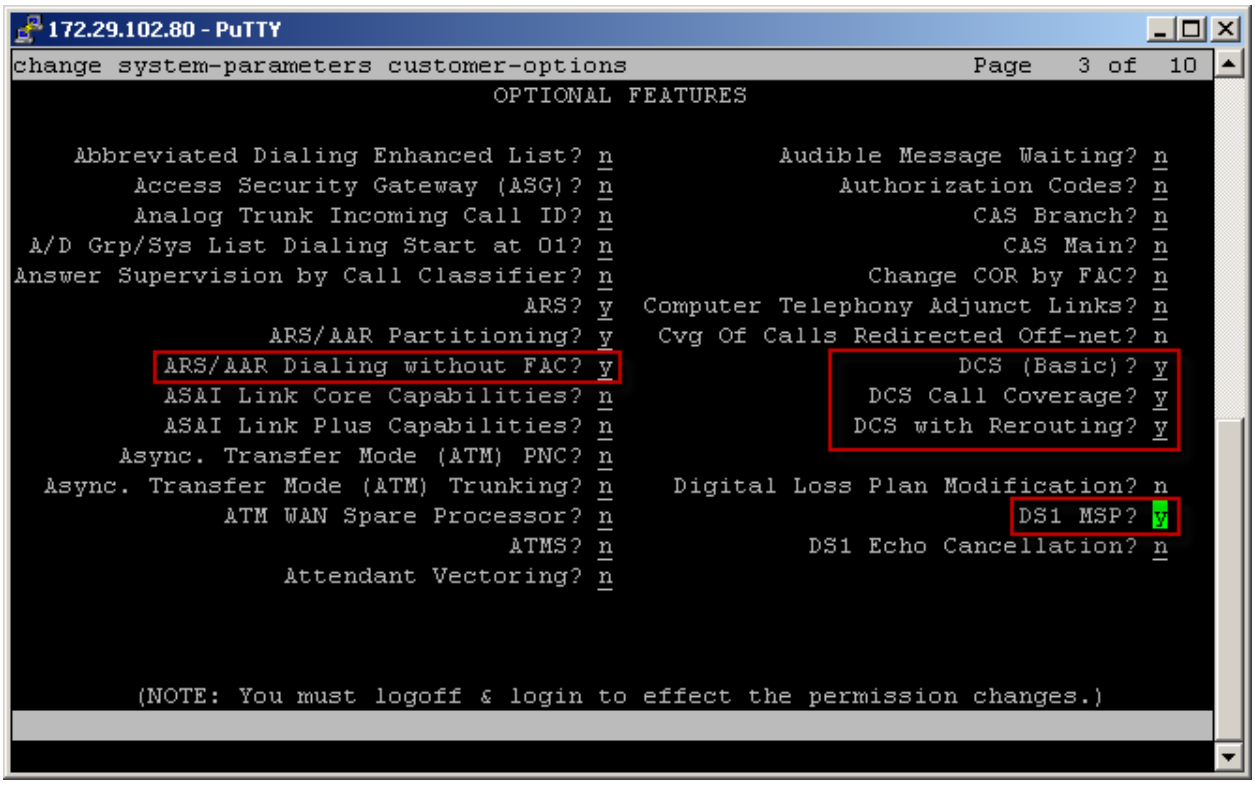
## *1. Q.SIG*

Q.SIG parameters are required.

**To set or confirm Q.SIG parameters:**

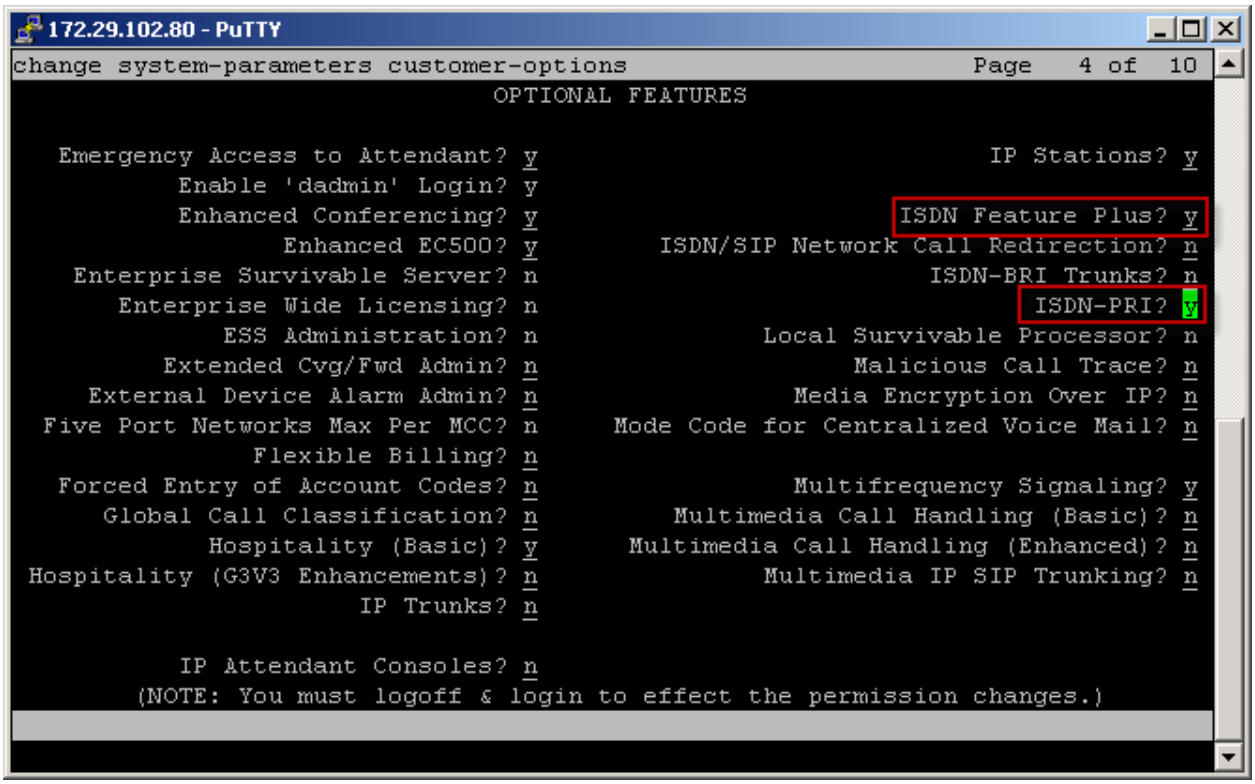
1. Login to the Avaya ACM and perform the display system-parameters customer-options command.
2. Go to page 3.
3. Ensure that these four fields are all set to a value of Yes. If not you will need to log back into the system using a login with sufficient permissions to change these, and modify them by performing a "change system-parameters customer-options". If you do not have access to change these and need to, you will need to contact a reseller.

| | |
|---|---|
| ARS/AAR Dialing without FAC | Y |
| DCS (Basic) | Y |
| DCS Call Coverage | Y |
| DCS with Rerouting | Y |
| DS1 MSP | Y |


172.29.102.80 - PuTTY
change system-parameters customer-options Page 3 of 10
OPTIONAL FEATURES
Abbreviated Dialing Enhanced List? n
Access Security Gateway (ASG)? n
Analog Trunk Incoming Call ID? n
A/D Grp/Sys List Dialing Start at 01? n
Answer Supervision by Call Classifier? n
ARS? y
ARS/AAR Partitioning? y
ARS/AAR Dialing without FAC? y
ASAI Link Core Capabilities? n
ASAI Link Plus Capabilities? n
Async. Transfer Mode (ATM) PNC? n
Async. Transfer Mode (ATM) Trunking? n
ATM WAN Spare Processor? n
ATMS? n
Attendant Vectoring? n
Audible Message Waiting? n
Authorization Codes? n
CAS Branch? n
CAS Main? n
Change COR by FAC? n
Computer Telephony Adjunct Links? n
Cvg Of Calls Redirected Off-net? n
DCS (Basic)? y
DCS Call Coverage? y
DCS with Rerouting? y
Digital Loss Plan Modification? n
DS1 MSP? y
DS1 Echo Cancellation? n
(NOTE: You must logoff & login to effect the permission changes.)

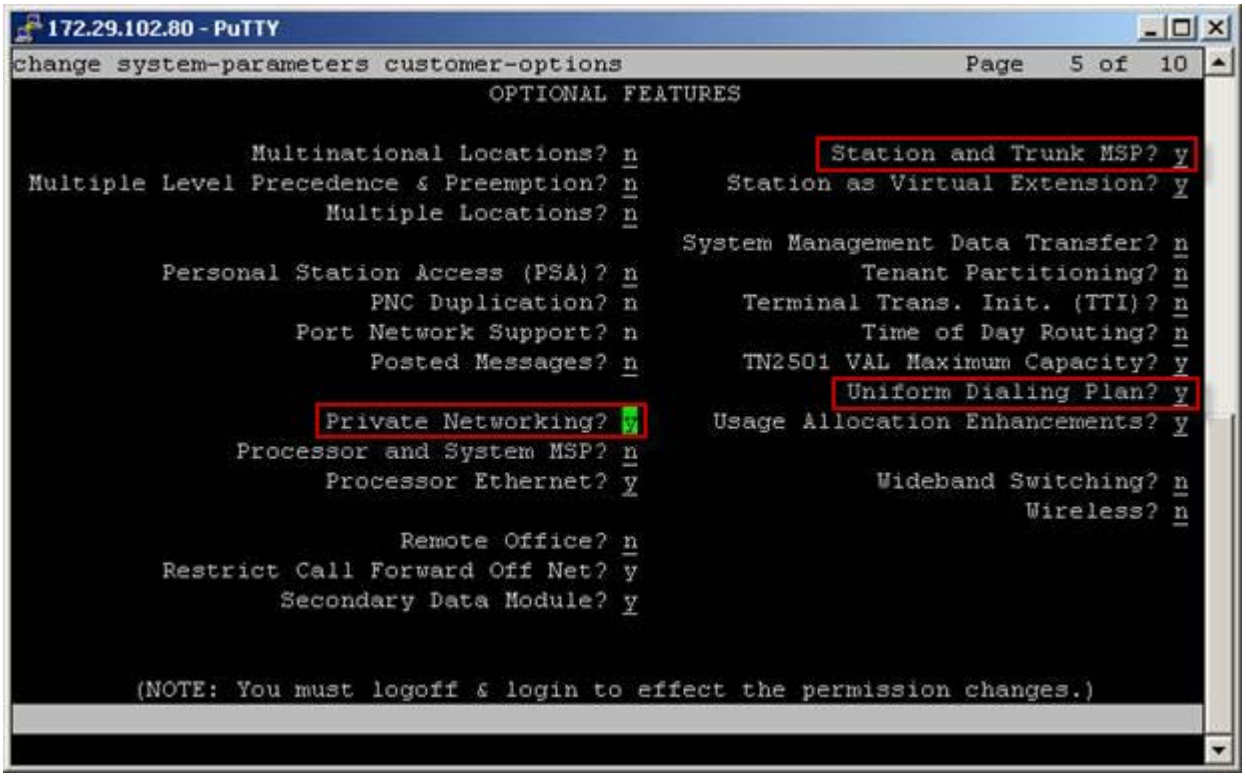
**4** On page 4 of the system-parameters customer-options screen ensure these fields are both set to a value of y:

| | |
|---|---|
| ISDN Feature Plus | Y |
| ISDN PRI | Y |

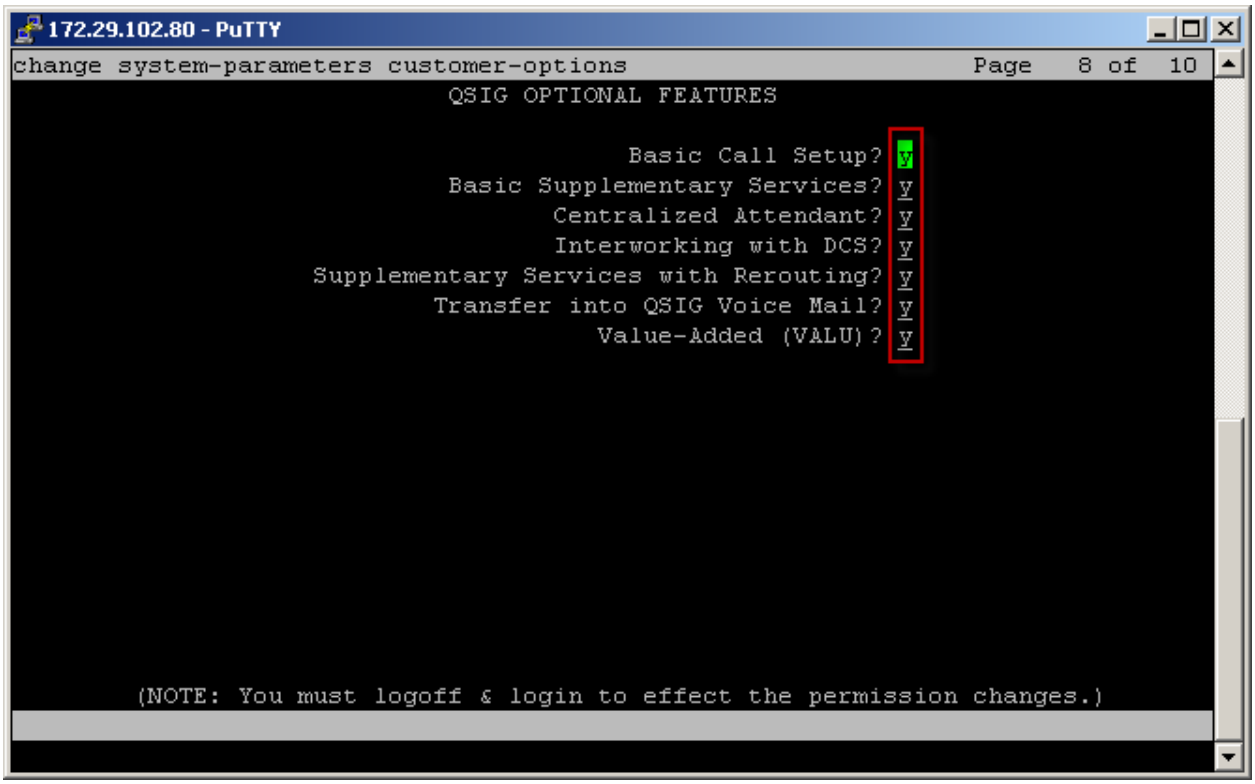

172.29.102.80 - PuTTY
change system-parameters customer-options Page 4 of 10
OPTIONAL FEATURES
Emergency Access to Attendant? y
IP Stations? y
Enable 'dadmin' Login? y
Enhanced Conferencing? y
ISDN Feature Plus? y
Enhanced EC500? y
ISDN/SIP Network Call Redirection? n
Enterprise Survivable Server? n
ISDN-BRI Trunks? n
Enterprise Wide Licensing? n
ISDN-PRI? y
ESS Administration? n
Local Survivable Processor? n
Extended Cvg/Fwd Admin? n
Malicious Call Trace? n
External Device Alarm Admin? n
Media Encryption Over IP? n
Five Port Networks Max Per MCC? n
Mode Code for Centralized Voice Mail? n
Flexible Billing? n
Forced Entry of Account Codes? n
Multifrequency Signaling? y
Global Call Classification? n
Multimedia Call Handling (Basic)? n
Hospitality (Basic)? y
Multimedia Call Handling (Enhanced)? n
Hospitality (G3V3 Enhancements)? n
Multimedia IP SIP Trunking? n
IP Trunks? n
IP Attendant Consoles? n
(NOTE: You must logoff & login to effect the permission changes.)

**5** On page 5 of the system-parameters customer-options screen ensure these fields are all set to a value of Yes:

| | |
|---|---|
| Station and Trunk MSP | Y |
| Uniform Dialing Plan | Y |
| Private Networking | Y |


172.29.102.80 - PuTTY
change system-parameters customer-options
Page 5 of 10
OPTIONAL FEATURES
Multinational Locations? n
Station and Trunk MSP? y
Multiple Level Precedence & Preemption? n
Station as Virtual Extension? y
Multiple Locations? n
System Management Data Transfer? n
Personal Station Access (PSA)? n
Tenant Partitioning? n
PNC Duplication? n
Terminal Trans. Init. (TTI)? n
Port Network Support? n
Time of Day Routing? n
Posted Messages? n
TN2501 VAL Maximum Capacity? y
Uniform Dialing Plan? y
Private Networking? y
Usage Allocation Enhancements? y
Processor and System MSP? n
Processor Ethernet? y
Wideband Switching? n
Wireless? n
Remote Office? n
Restrict Call Forward Off Net? y
Secondary Data Module? y
(NOTE: You must logoff & login to effect the permission changes.)

**6** On page 8 of the system-parameters customer-options screen ensure all of the fields are set to a value of Yes:


172.29.102.80 - PuTTY
change system-parameters customer-options Page 8 of 10
QSIG OPTIONAL FEATURES
Basic Call Setup? y
Basic Supplementary Services? y
Centralized Attendant? y
Interworking with DCS? y
Supplementary Services with Rerouting? y
Transfer into QSIG Voice Mail? y
Value-Added (VALU)? y
(NOTE: You must logoff & login to effect the permission changes.)

**7** Press Esc-E to submit.

**Admin Tip**

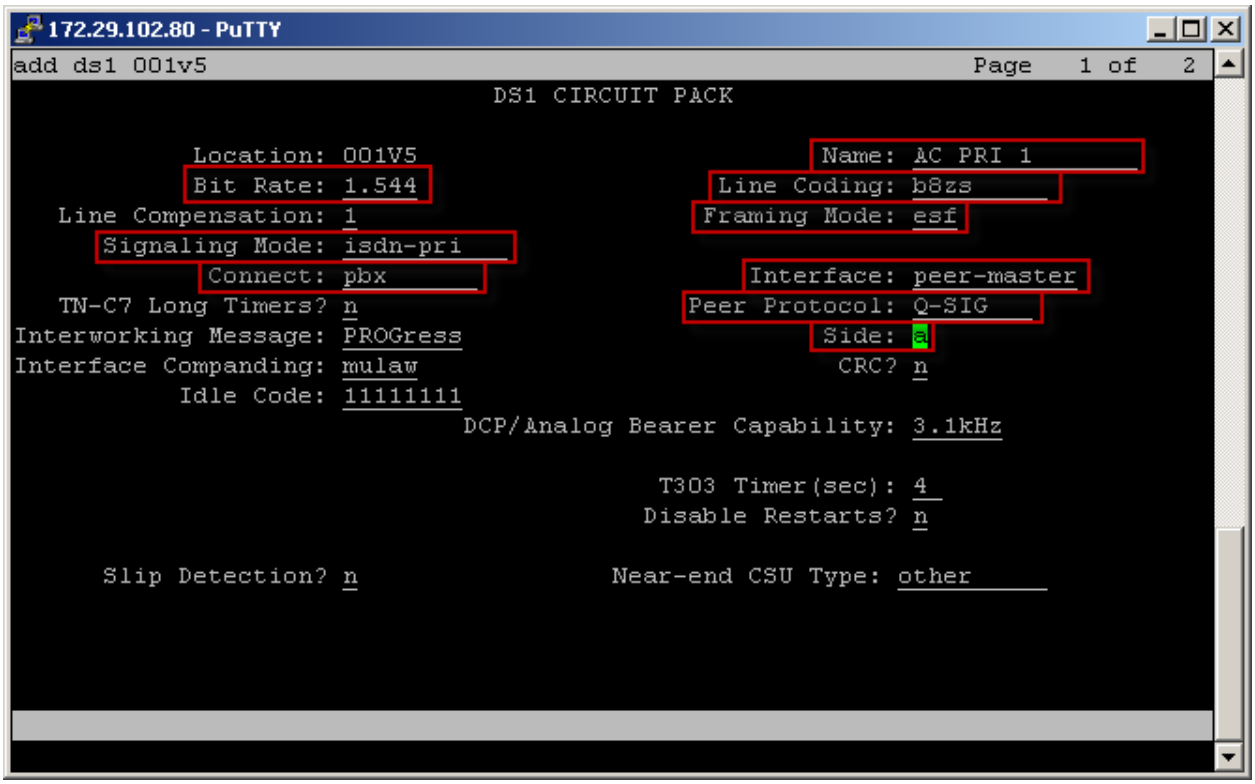
If you made changes you will need to logoff and log back in to effect the changes.

# 2. Add or Change the DS1 to Support Q.SIG

**1** Enter *add ds1 xxxxx* command, where xxxxx is the carrier/slot location of the DS1 connected to the Mediant 1000. For this configuration 001v5 was used.

**2** On page 1 of the ds1 form configure the following:

| | |
|---|---|
| Name | Enter something meaningful |
| Bit Rate | 1.544 |
| Line Coding | b8zs |
| Framing Mode | esf |
| Signaling Mode | isdn-pri |
| Connect | PBX |
| Interface | peer-master |
| Peer Protocol | Q-SIG |
| Side | Set to a |




**3** Press Esc-E to submit.

# 3. Add Signaling Group to Trunk Group

Create a signaling group for the trunks and put it into the Mediant Gateway trunk group. We used signaling group #2 for this test. You can choose any available signaling group number.

**1** Use the command *add signaling-group x*, where x is the number of the signaling group you wish to add.

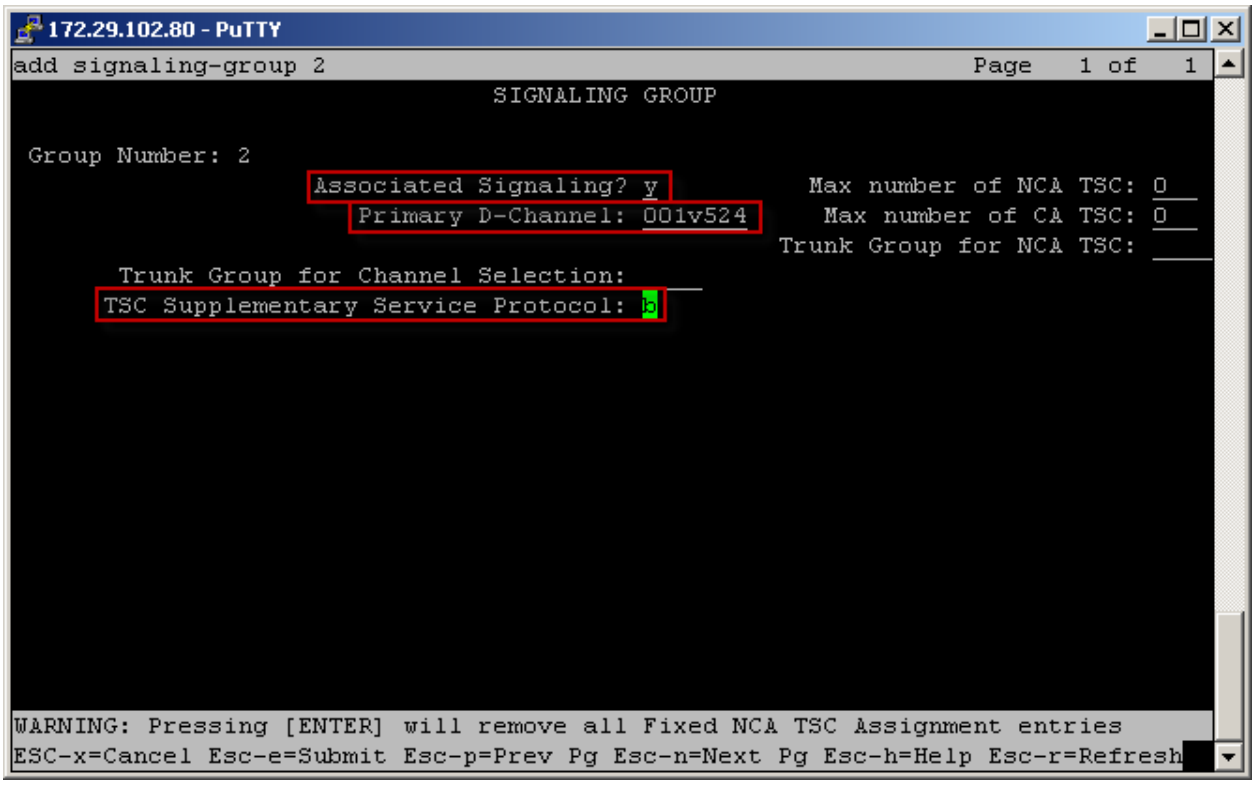
**Note: What are the existing signaling groups?**

You can view the existing signaling-groups by executing a *list signaling-group* command.

**2** (Conditional) If you have a Group Type field, set it to isdn-pri. This field was not available in the 5.2 system but may be available on other system versions.

**3** Configure the following

| | |
|---|---|
| Associated Signaling | y |
| Primary D Channel | Enter xxxxx24, where xxxxx is the location of the DS1 media module configured above. |
| TSC Supplementary Service Protocol | b |


172.29.102.80 - PuTTY
add signaling-group 2
Page 1 of 1
SIGNALING GROUP
Group Number: 2
Associated Signaling? y
Max number of NCA TSC: 0
Primary D-Channel: 001v524
Max number of CA TSC: 0
Trunk Group for NCA TSC:
Trunk Group for Channel Selection:
TSC Supplementary Service Protocol: b
WARNING: Pressing [ENTER] will remove all Fixed NCA TSC Assignment entries
ESC-x=Cancel Esc-e=Submit Esc-p=Prev Pg Esc-n=Next Pg Esc-h=Help Esc-r=Refresh

**4** Press Esc-E to submit.

# 4. Add a Trunk Group

The next step is to add a trunk group for our trunk connections to the Mediant Mediant Gateway . For this test, we used trunk group 2 for the Q.SIG trunk to the Mediant 1000.

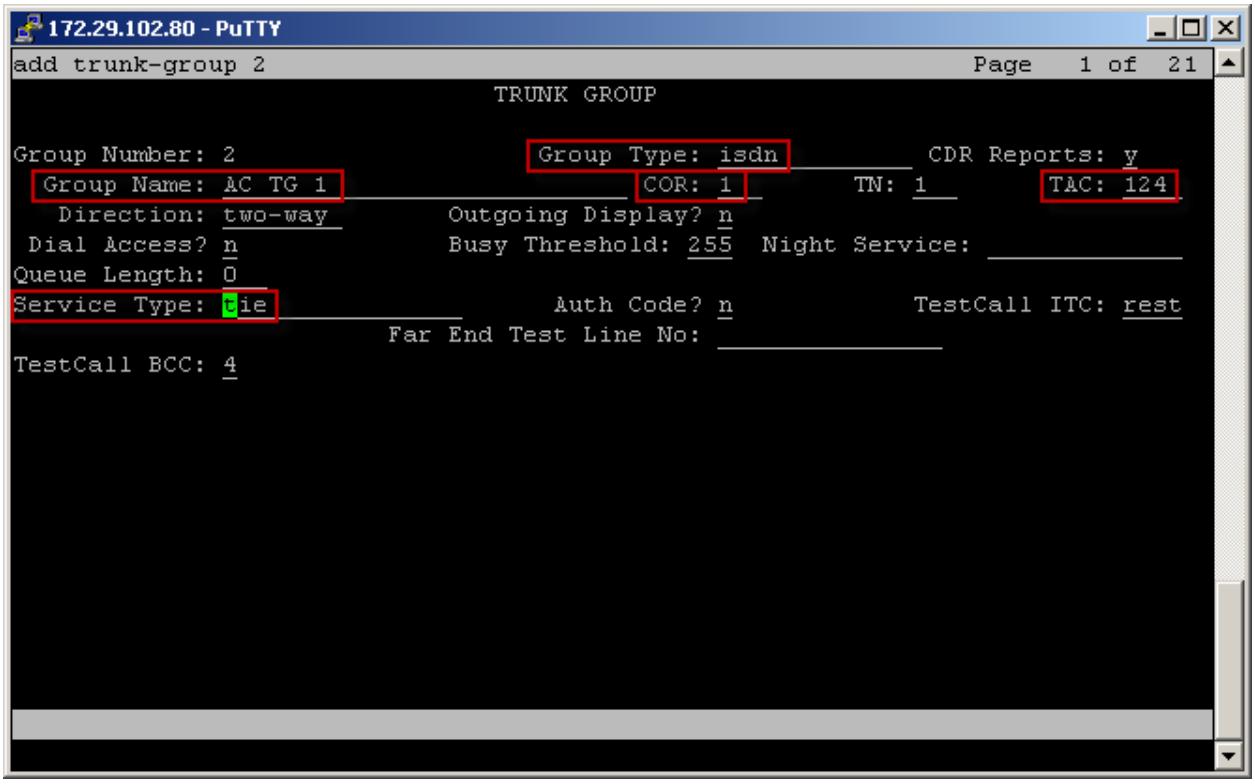
**Note: What are the existing signaling groups?**

You can view the existing signaling-groups by executing a *list signaling-group* command.

1. Enter the *add trunk-group x* command, where x is an available trunk group number.
2. On page 1 of the trunk group form, configure the following:

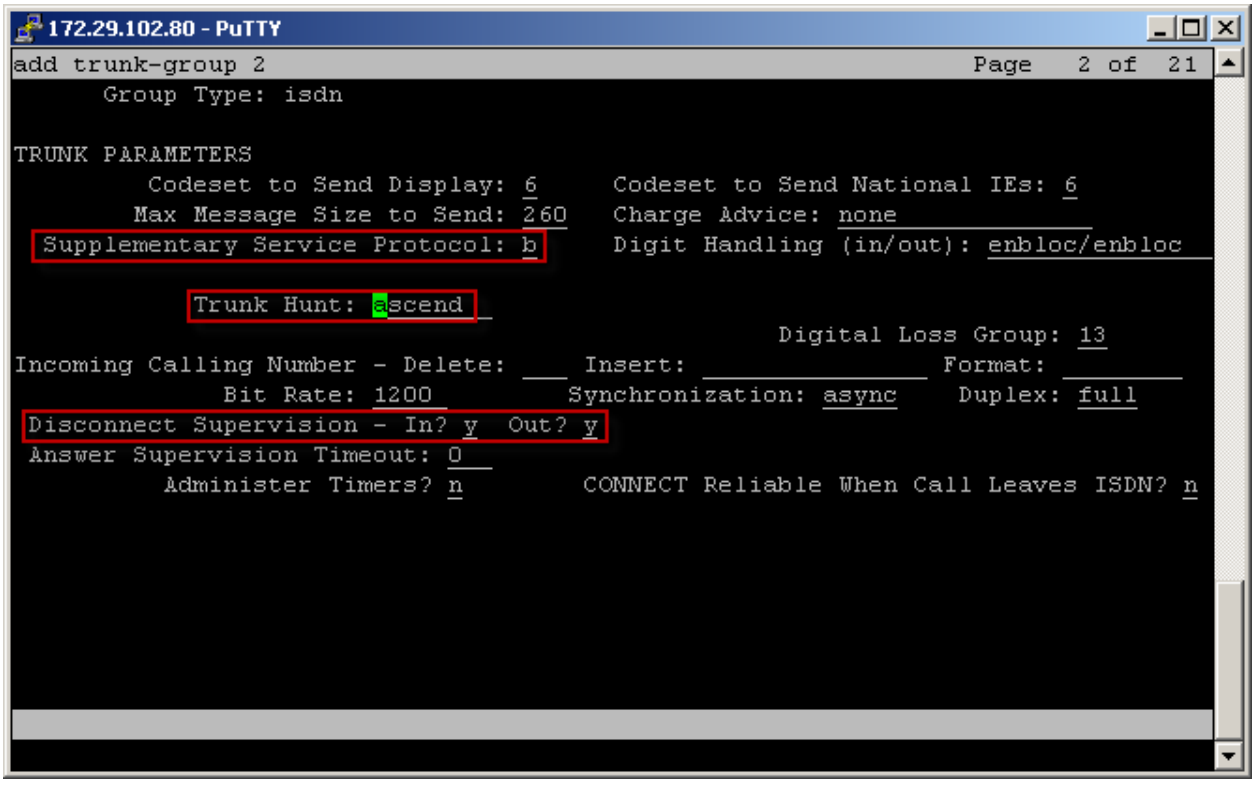
| | |
|---|---|
| Group Type | isdn. |
| Group Name | Enter a meaningful name |
| TAC | Enter a Trunk Access Code that does not conflict with the existing dialing plan |
| COR | Enter a class of restriction that will allow trunk to trunk transfers (for purposes of this example COR 1 is unrestricted) |
| Service Type | tie |

3. (Conditional) If you have a Carrier Medium field, set it to PRI/BRI. This field was not available in the 5.2 system but may be available on other system versions.



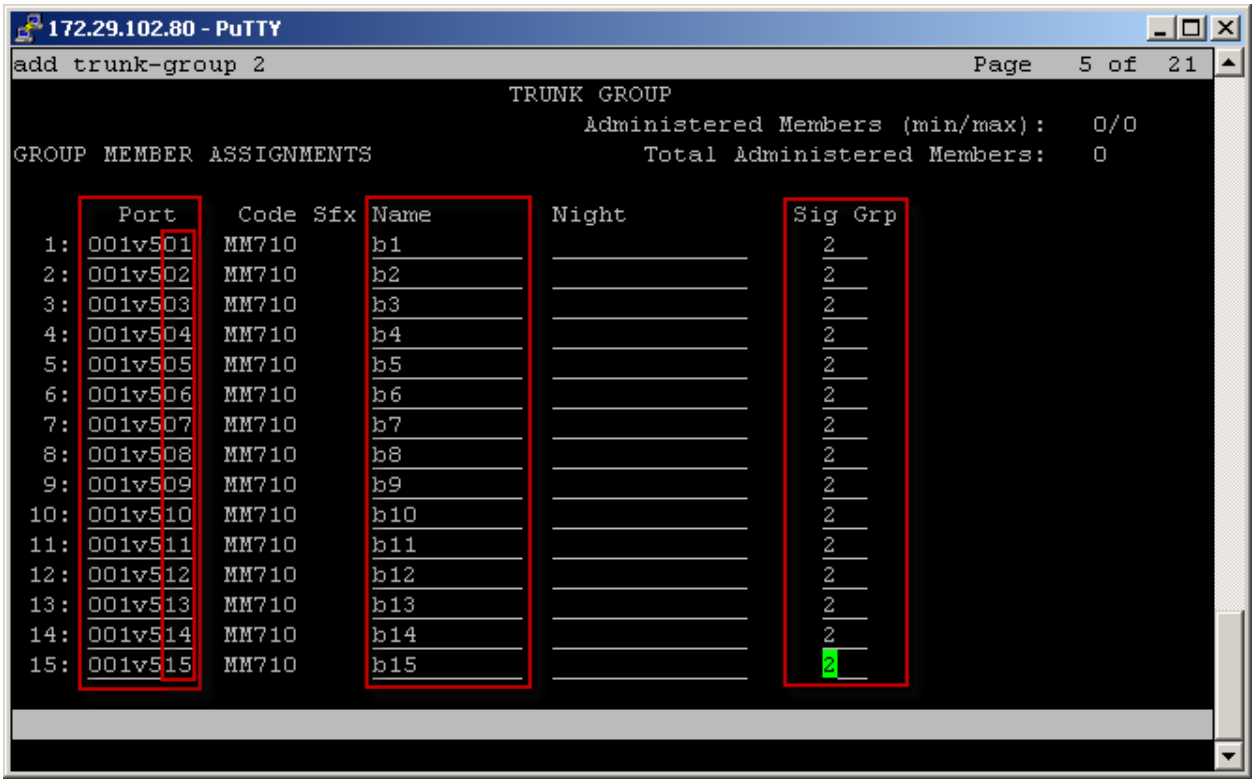
**4** On page 2 of the trunk group form, ensure:

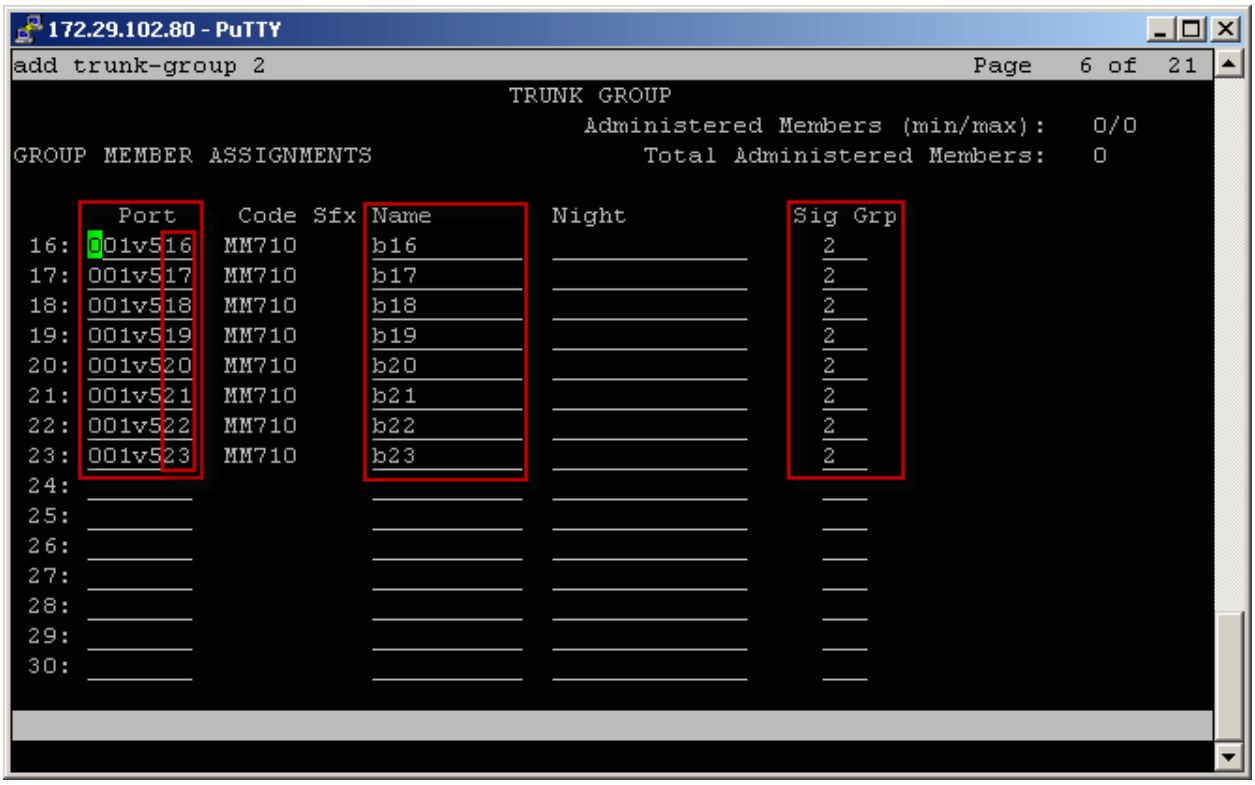
| | |
|---|---|
| Supplementary Service Protocol | b |
| Trunk Hunt | ascend (note that we set the Mediant Gateway to descending so as to reduce the possibility of "glare") |
| Disconnect Supervision | yes for both In? and Out? |


172.29.102.80 - PuTTY
add trunk-group 2 Page 2 of 21
Group Type: isdn
TRUNK PARAMETERS
Codeset to Send Display: 6 Codeset to Send National IEs: 6
Max Message Size to Send: 260 Charge Advice: none
Supplementary Service Protocol: b Digit Handling (in/out): enbloc/enbloc
Trunk Hunt: ascend
Digital Loss Group: 13
Incoming Calling Number - Delete: Insert: Format:
Bit Rate: 1200 Synchronization: async Duplex: full
Disconnect Supervision - In? y Out? y
Answer Supervision Timeout: 0
Administer Timers? n CONNECT Reliable When Call Leaves ISDN? n

**5** On pages 5 and 6, enter the Individual trunks for channels 1-23.

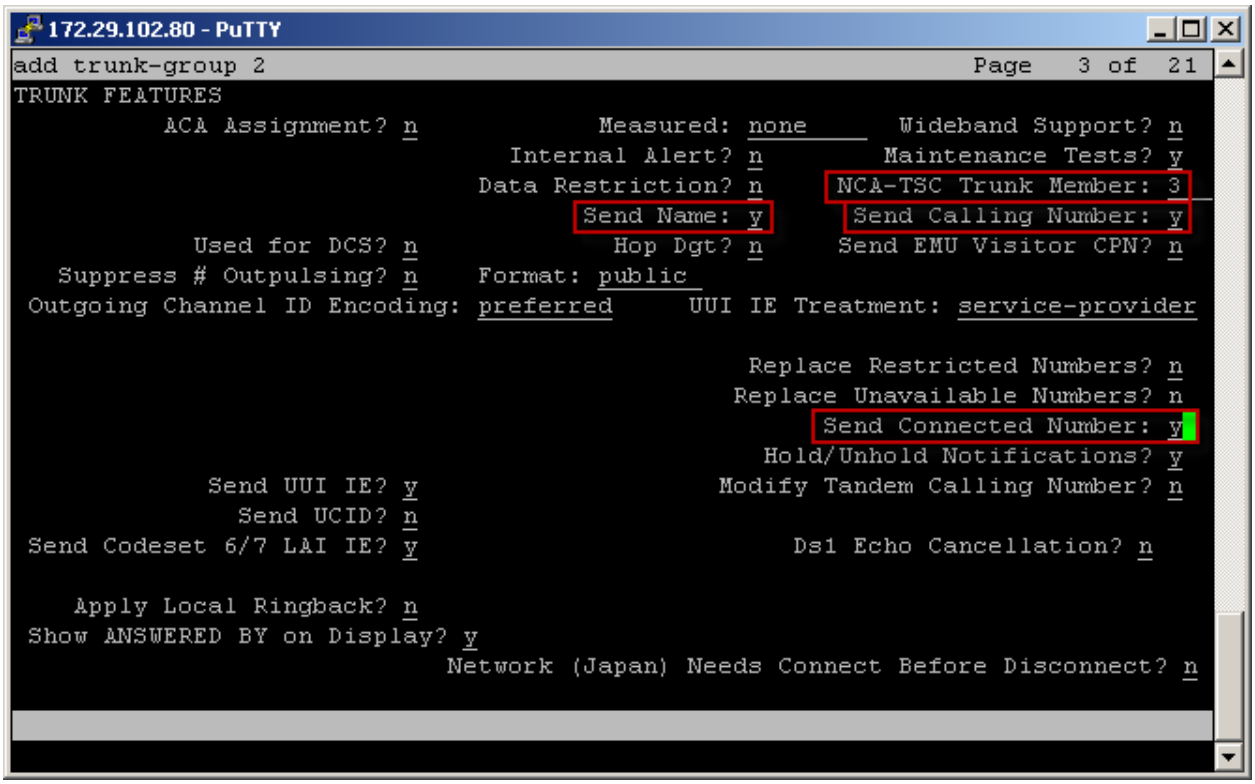
| | |
|---|---|
| Port | The port number should correspond with the slot location you entered for the T1/ PRI, followed by the individual trunk number (1-23). |
| Code | This field should auto-populate with the media module type that is supporting the PRI. |
| Name | In this example, these were named b1 through b23. You can use whatever you'd like. |
| Signaling Group | Enter the Signaling Group number you created above. |



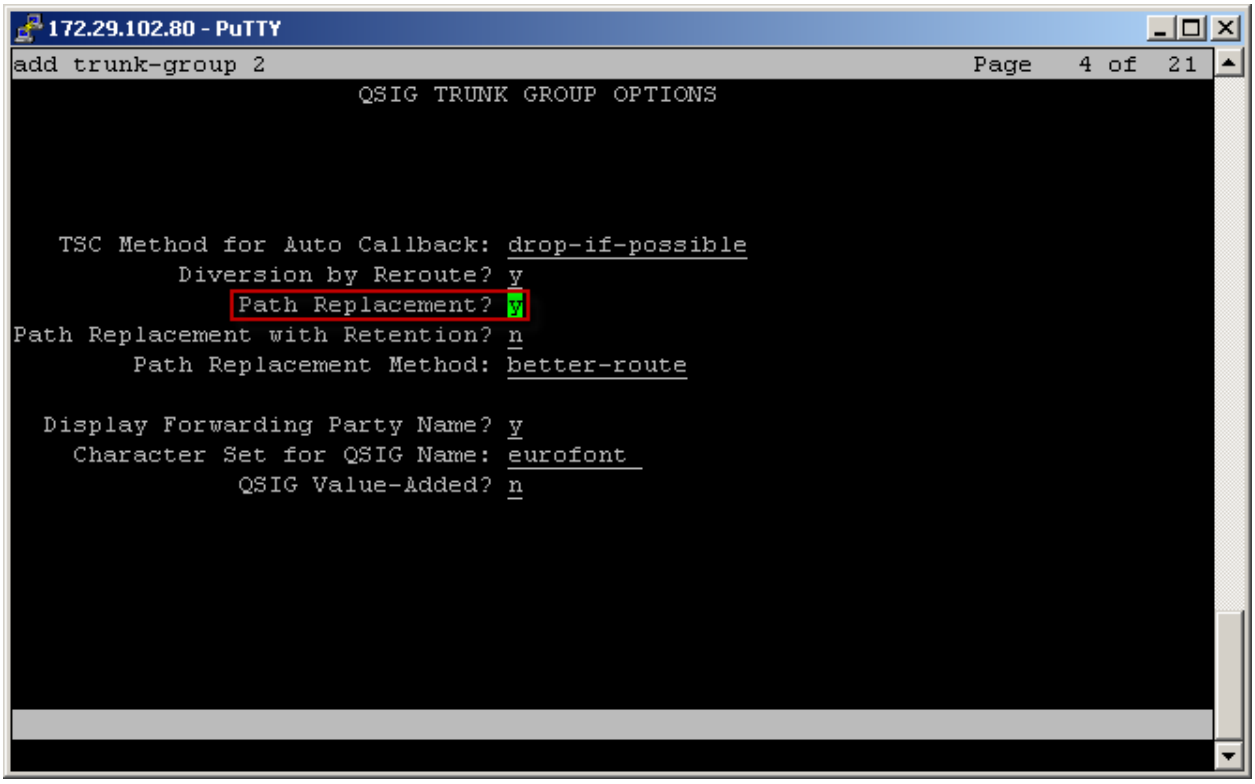

172.29.102.80 - PuTTY
add trunk-group 2
Page 6 of 21
TRUNK GROUP
Administered Members (min/max): 0/0
GROUP MEMBER ASSIGNMENTS
Total Administered Members: 0
Port
Code
Sfx
Name
Night
Sig Grp
16: 001v516 MM710 b16 2
17: 001v517 MM710 b17 2
18: 001v518 MM710 b18 2
19: 001v519 MM710 b19 2
20: 001v520 MM710 b20 2
21: 001v521 MM710 b21 2
22: 001v522 MM710 b22 2
23: 001v523 MM710 b23 2
24:
25:
26:
27:
28:
29:
30:

**6** On page 3, set the following

| | |
|---|---|
| NCA-TSC Trunk Member | Set this to one of the Trunk Members (1-23) |
| Send Name | y |
| Send Calling Number | y |
| Send Connected Number | y |


172.29.102.80 - PuTTY
add trunk-group 2 Page 3 of 21
TRUNK FEATURES
ACA Assignment? n Measured: none Wideband Support? n
Internal Alert? n Maintenance Tests? y
Data Restriction? n NCA-TSC Trunk Member: 3
Send Name: y Send Calling Number: y
Used for DCS? n Hop Dgt? n Send EMU Visitor CPN? n
Suppress # Outpulsing? n Format: public
Outgoing Channel ID Encoding: preferred UUI IE Treatment: service-provider
Replace Restricted Numbers? n
Replace Unavailable Numbers? n
Send Connected Number: y
Hold/Unhold Notifications? y
Send UUI IE? y Modify Tandem Calling Number? n
Send UCID? n
Send Codeset 6/7 LAI IE? y Ds1 Echo Cancellation? n
Apply Local Ringback? n
Show ANSWERED BY on Display? y
Network (Japan) Needs Connect Before Disconnect? n

**7** On page 4 ensure that Path Replacement is set to y

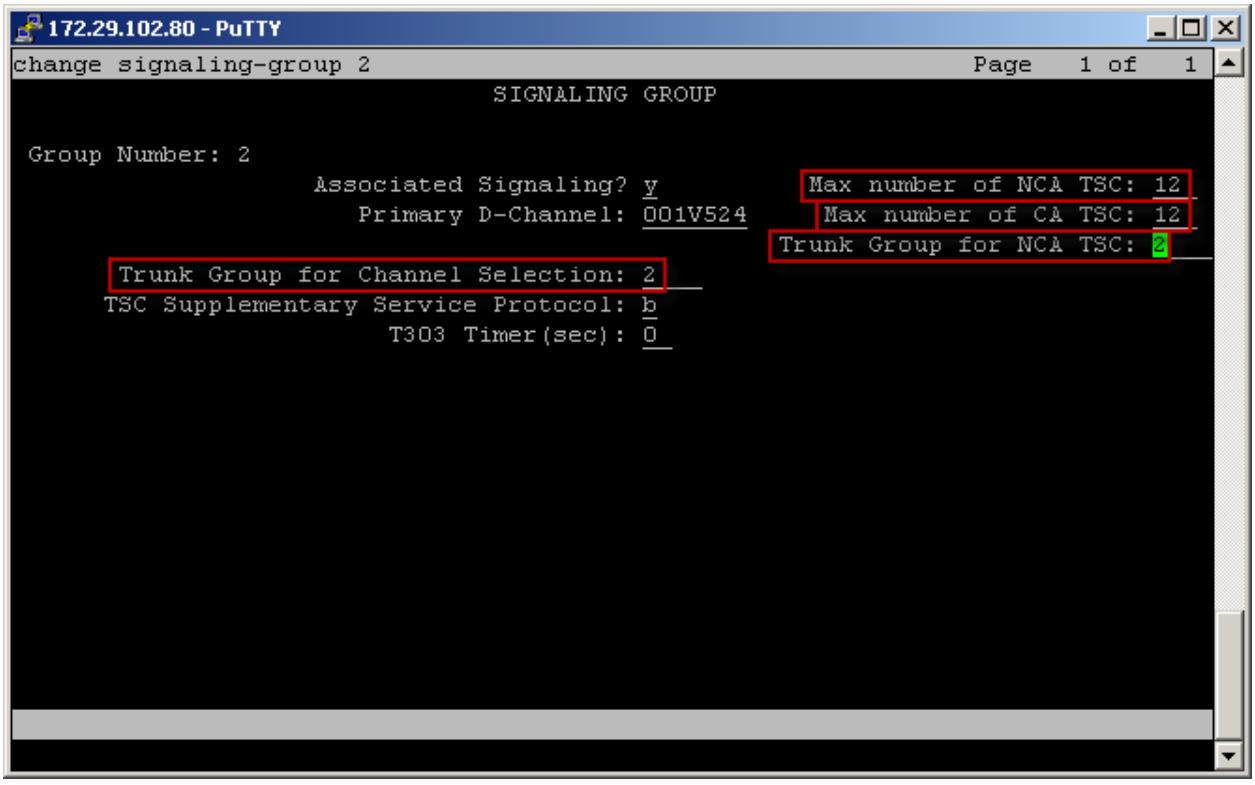

172.29.102.80 - PuTTY
add trunk-group 2
Page 4 of 21
QSIG TRUNK GROUP OPTIONS
TSC Method for Auto Callback: drop-if-possible
Diversion by Reroute? y
Path Replacement? y
Path Replacement with Retention? n
Path Replacement Method: better-route
Display Forwarding Party Name? y
Character Set for QSIG Name: eurofont
QSIG Value-Added? n

# 5. Change Signaling Group

Now we must go back and change the signaling group. You might say "Why didn't we just add these fields to the signaling group when we created it?" Unfortunately, we have a bit of a chicken and egg problem. We can't select the trunk group for channel selection until we've created the trunk group, but we can't create the trunk group without specifying the signaling group that the trunk members will use.

1. Enter the command *change signaling-group x*, where x is the signaling group number you created above when you modified the signaling group.
2. Change the following fields:

| | |
|---|---|
| Trunk Group for Channel Selection | Enter the number of the trunk group configured in Step 3 |
| Max Number of NCA | TSC: 12 |
| Max Number of CA TSC | 12 |
| Trunk Group for NCA- TSC | Enter the number of the Trunk Group configured in Step 4. |

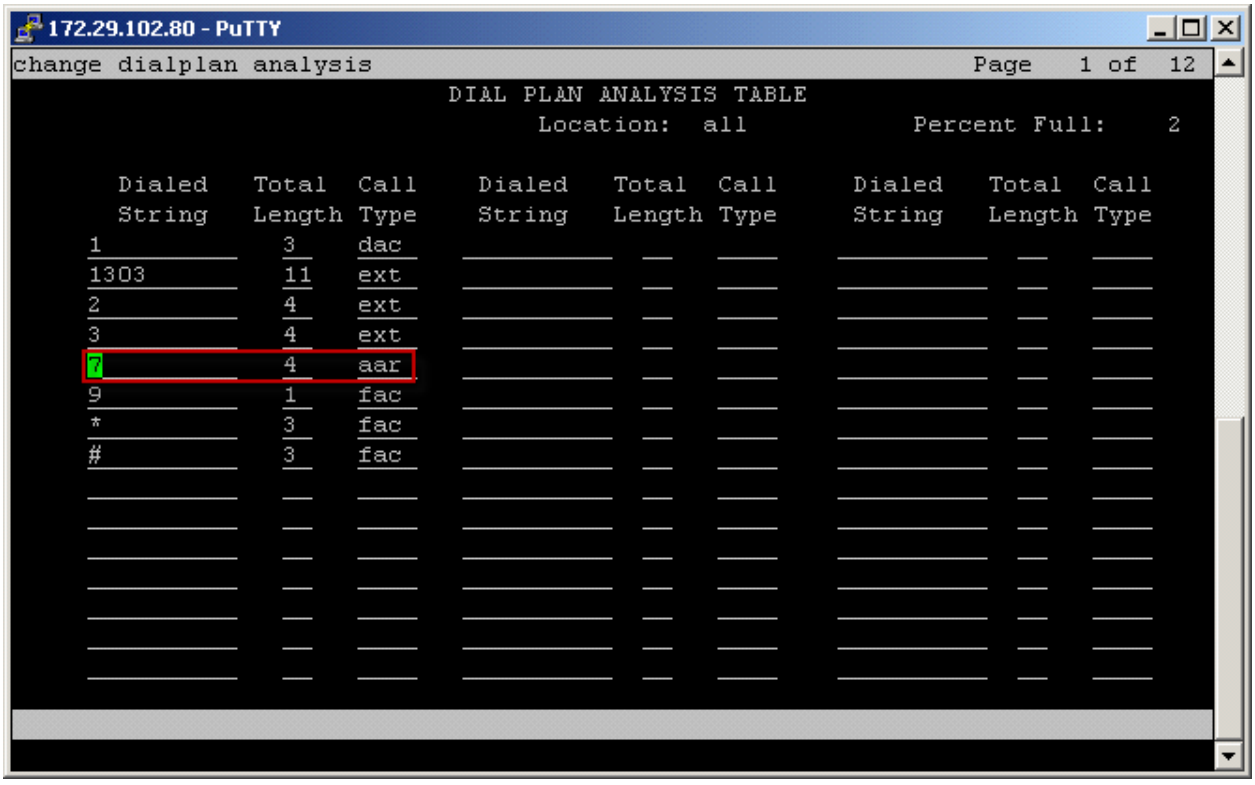

172.29.102.80 - PuTTY
change signaling-group 2
Page 1 of 1
SIGNALING GROUP
Group Number: 2
Associated Signaling? y
Primary D-Channel: 001V524
Max number of NCA TSC: 12
Max number of CA TSC: 12
Trunk Group for NCA TSC: 2
Trunk Group for Channel Selection: 2
TSC Supplementary Service Protocol: b
T303 Timer(sec): 0

# 6. Set up Dialing Parameters

Now we need a way to send calls intended for stations connected to the Mediant Gateway out the PRI. There are many ways to setup a dialplan in an Avaya system and detailing all of them is beyond the scope of this document. For our example we will assume that all calls intended for stations with a pattern of 70xx as their extension number will be sent out the PRI to the AudioCodes Mediant Gateway .

First, we need to ensure that the number range we wish to use is defined as a number we want the system to look at the aar analysis tables to decide how to route.

1. Enter the command change dialplan analysis.
2. For extensions with the format 7xxx, add a string to tell them to look at the aar table for information on which trunk group and route patterns to use to route the call.



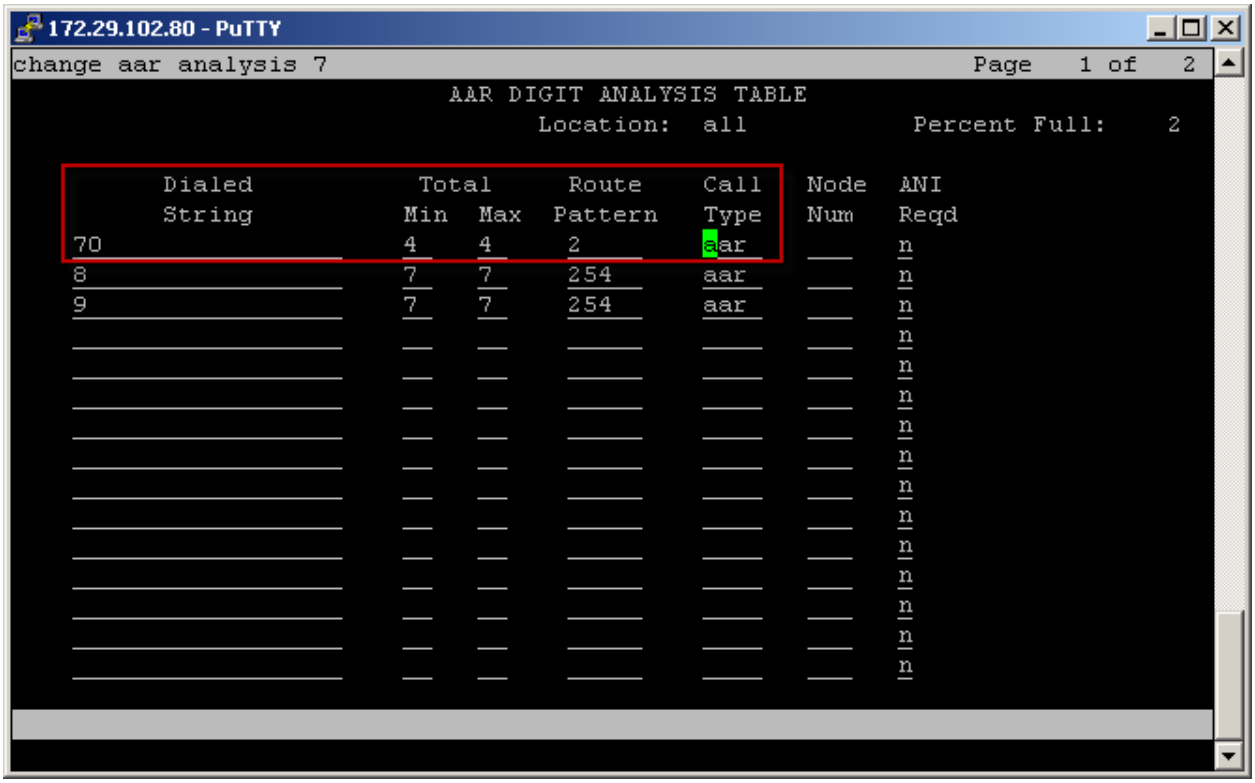
# 7. Change the Automatic Alternate Routing Table

Next we want to change the Automatic Alternate Routing table to tell the system that anytime someone dials 70xx, we want to send that call out the PRI to the AudioCodes Mediant Gateway.

**1** Enter the command *change aar analysis x*.

**2** Add these parameters:

| | |
|---|---|
| Dialed String | Enter as much of the unique pattern as you can easily define. If I wanted all 7xxx numbers to go out this PRI, I would just use a 7. If all calls to 701x were to go out this PRI I would use 701. This test used 70. |
| Total Min and Max | Enter the total number of digits in the extensions' length |
| Route Pattern | Enter a unique number which will be used to create the route pattern in the next step. If you are unsure, cancel the current command and use the command *list route pattern.* Then define the next available number. |
| Call Type | aar |



# 8. Add the Route Pattern

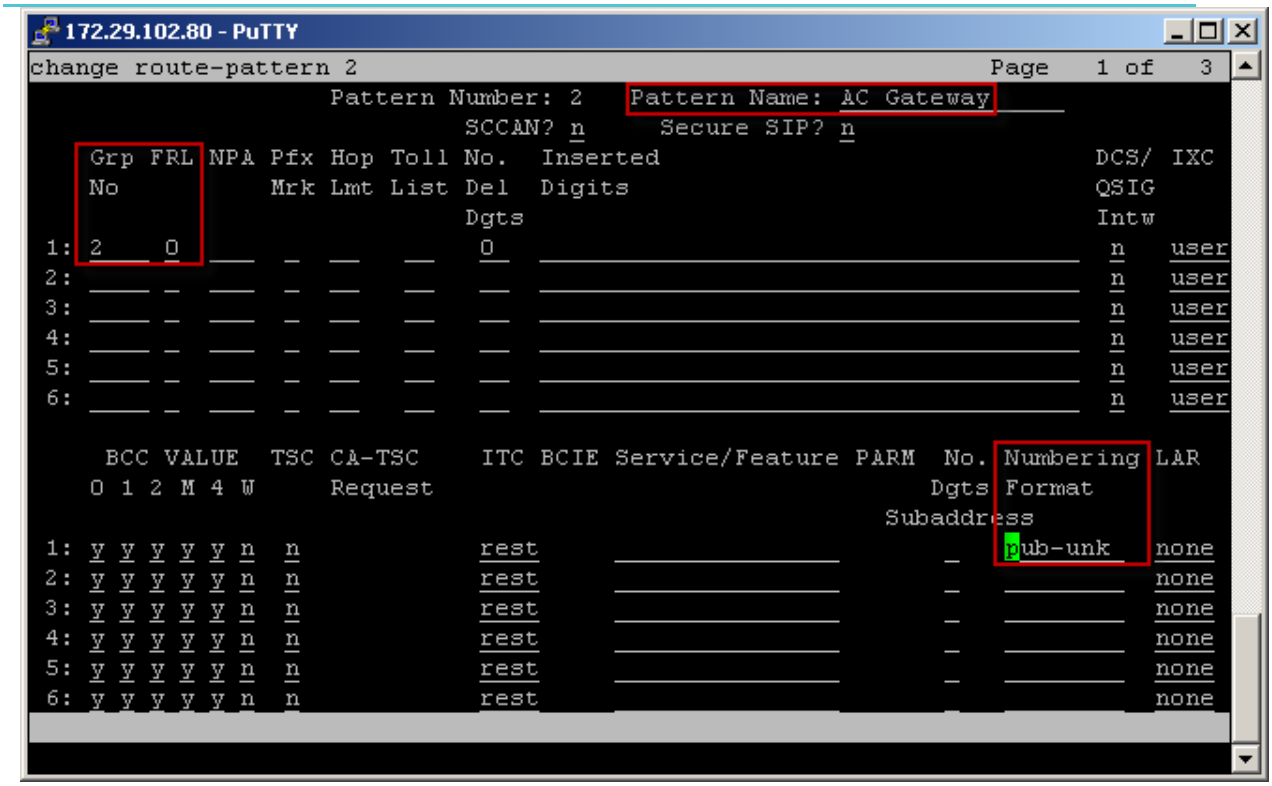
**Note: What are the existing route patterns?**

If some route patterns already exist in the system you would use the command *change route pattern x*.

1 Enter the command *add route-pattern x*, where x is the number of the unique route pattern you created in step 7 (In the test case 2 was used).

2 Set these parameters:

| | |
|---|---|
| Name | Enter a meaningful name. The test used AC_Mediant Gateway |
| Group Number | Enter the Trunk Group Number you created in Step 4 (Mine is TG #2) |
| FRL | Choose a facility restriction level that will not compromise your sites' security practices |
| Numbering Format | pub-unk |




3 Press Esc-E to submit.

**Note: Test the configuration**

If you are not adding multiple T1's / PRI's, then your configuration should be complete at this point and you should skip forward to the testing section to verify functionality.

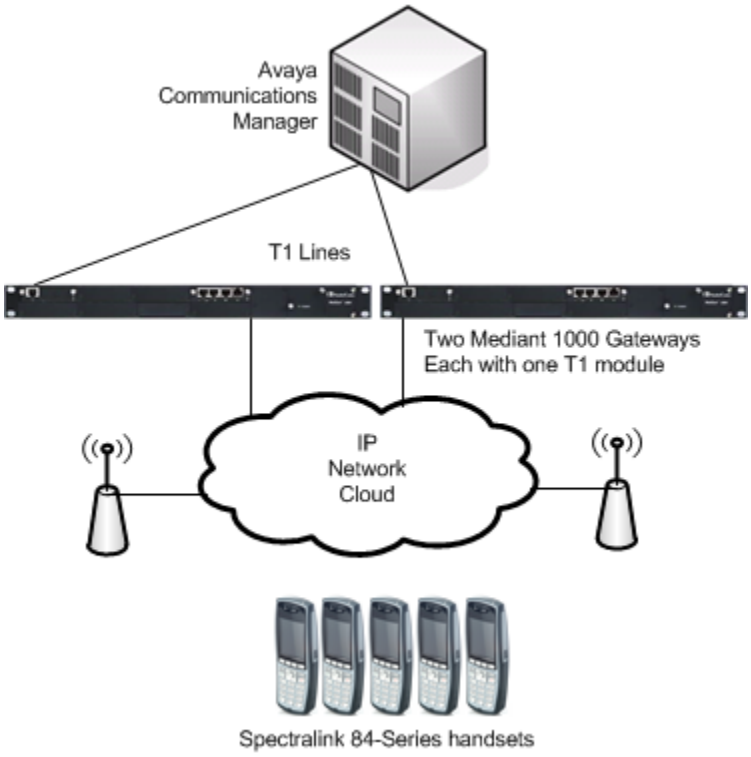
# Chapter 10: Expanding your System

## *Adding a Second Trunk Group on the Same PBX*

One method of expansion is to simply add another Mediant Gateway with one T1 module. This section covers the configuration of the two-Mediant Gateway system.

**Admin Tip: Configuring the second Mediant Gateway**

In this configuration, the second Mediant Gateway is configured just like the first one. Only PBX changes are needed.



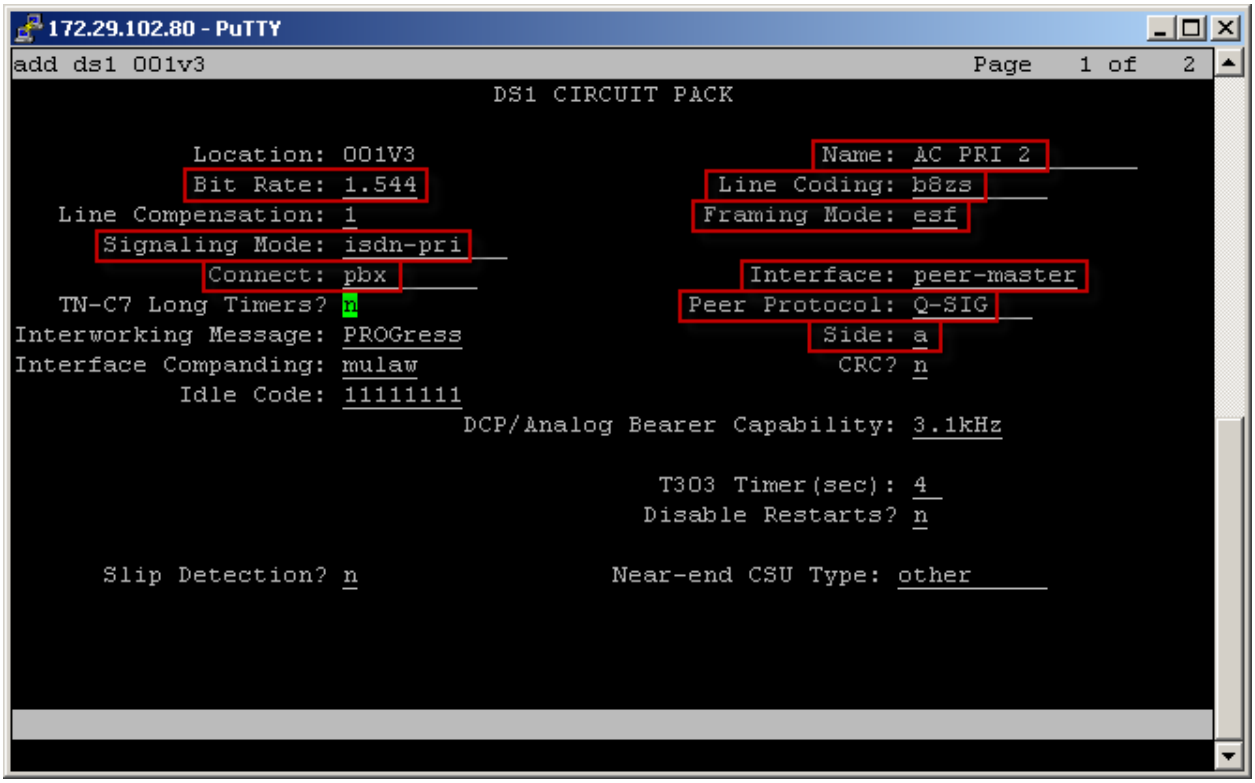

**Admin Tip: Allocate a second PRI card in the PBX**

You will need to install or allocate a second PRI card in the PBX for this configuration.

## 1. Add another DS1

**1** Enter *add ds1 xxxxx command*, where xxxxx is the carrier/slot location of the DS1 connected to the Mediant 1000. For this configuration 001v3 was used. On page 1 of the ds1 form configure the following:

| | |
|---|---|
| Name | Enter something meaningful |
| Bit Rate | 1.544 |
| Line Coding | b8zs |
| Frame mode | esf |
| Signaling Mode | isdn-pri |
| Connect | PBX |
| Interface | peer-master |
| Peer Protocol | Q-SIG |
| Side | a |




**2** Press Esc-E to submit.

## 2. Add Signaling Group

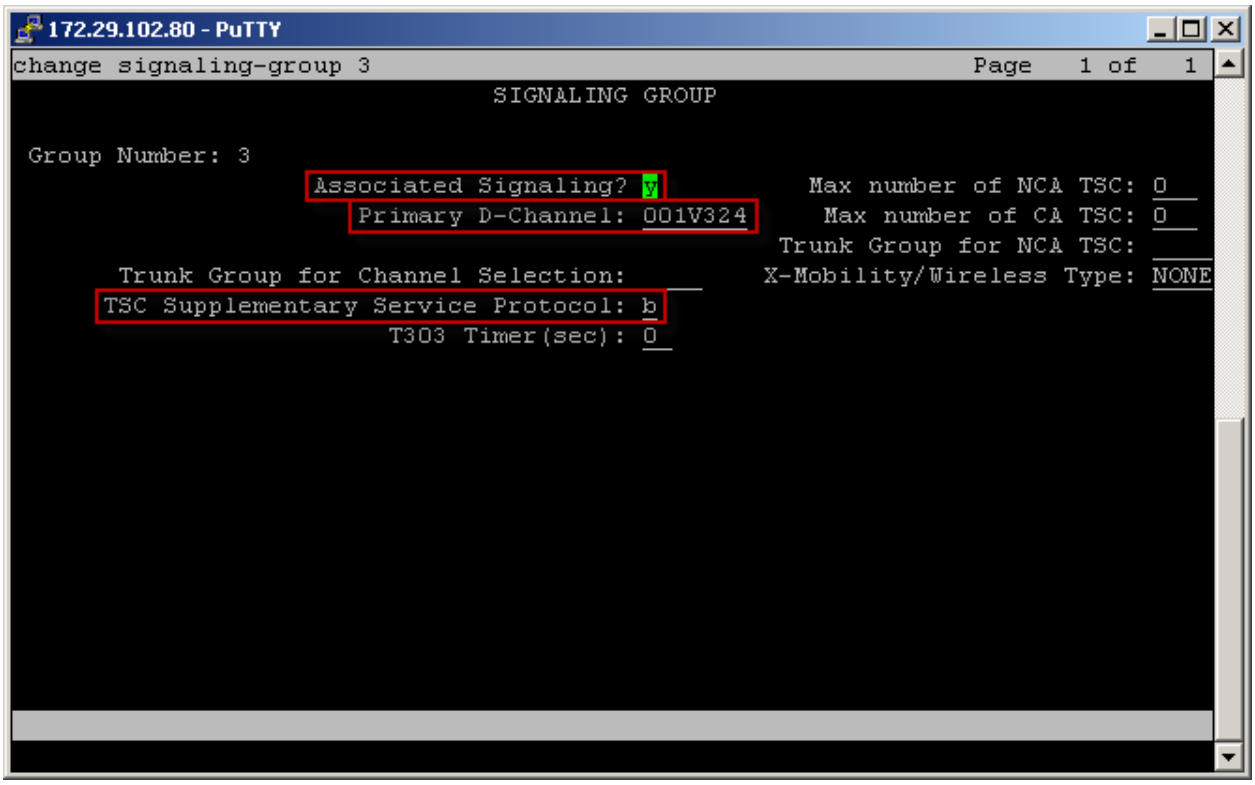
**1** Enter the command *add signaling-group x*, where x is the number of the signaling group you wish to add.

**Note: What are the existing signaling groups?**

You can view the existing signaling-groups by executing a *list signaling-group* command.

**2** (Conditional) If you have a Group Type field, set it to isdn-pri. This field was not available in the 5.2 system but may be available on other system versions.

| | |
|---|---|
| Associated Signaling | y |
| Primary D Channel | Enter xxxxx24, where xxxxx is the location of the DS1 media module configured above. |
| TSC Supplementary Service Protocol | b |




**3** Press Esc-E to submit.

## 3. Add a Trunk Group

The next step is to add a trunk group for our trunk connections to the Mediant Mediant Gateway. For this test, we used trunk group 3 for the Q.SIG trunk to the Mediant 1000.

**Note: What are the existing signaling groups?**

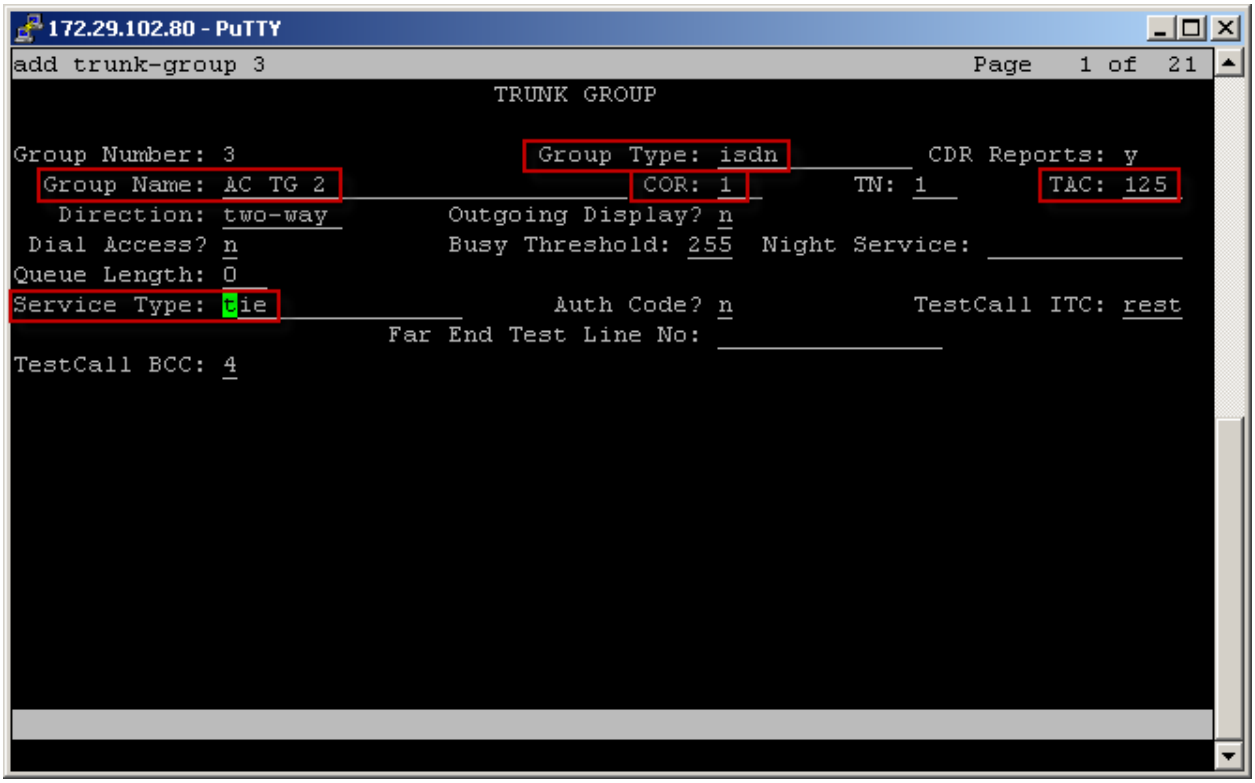
You can view the existing signaling-groups by executing a *list signaling-group* command.

**1** Enter the *add trunk-group x* command, where x is an available trunk group number.

**2** On page 1 of the trunk group form, configure the following:

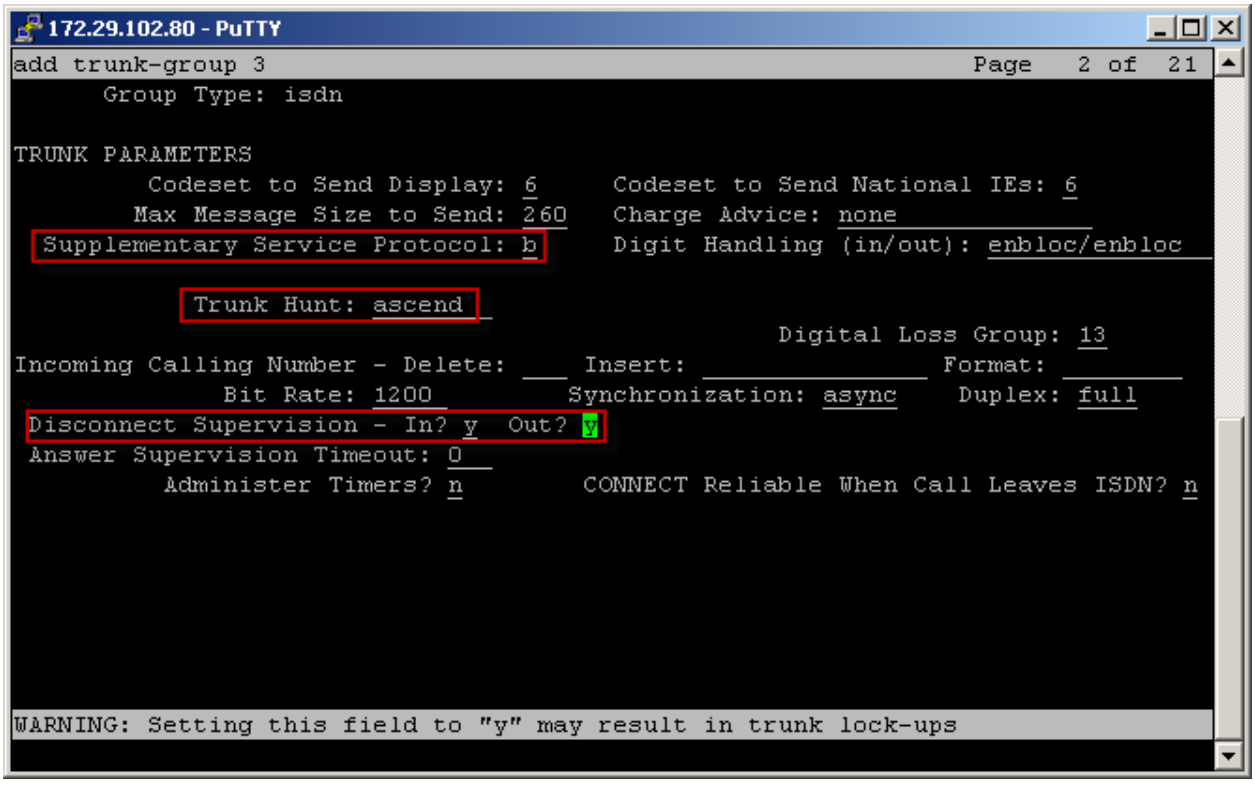
| | |
|---|---|
| Group Type | isdn. |
| Group Name | Enter a meaningful name |
| TAC | Enter a Trunk Access Code that does not conflict with the existing dialing plan |
| COR | Enter a class of restriction that will allow trunk to trunk transfers (for purposes of this example COR 1 is unrestricted) |
| Service Type | tie |

**3** (Conditional) If you have a Carrier Medium field, set it to PRI/BRI. This field was not available in the 5.2 system but may be available on other system versions.



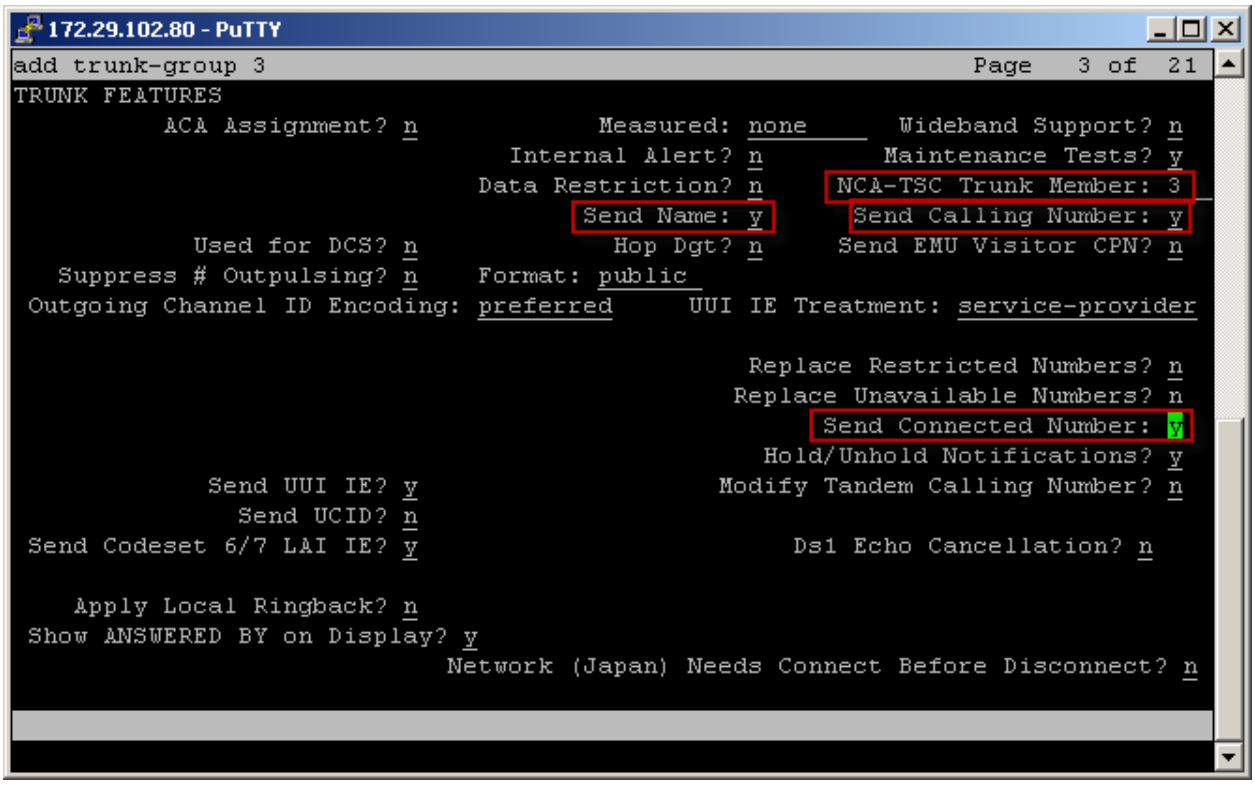

**4** On page 2 of the trunk group form, ensure:

| | |
|---|---|
| Supplementary Service Protocol | b |
| Trunk Hunt | ascend (note that we set the Mediant Gateway to descending so as to reduce the possibility of "glare") |
| Disconnect Supervision | yes for both In? and Out? |

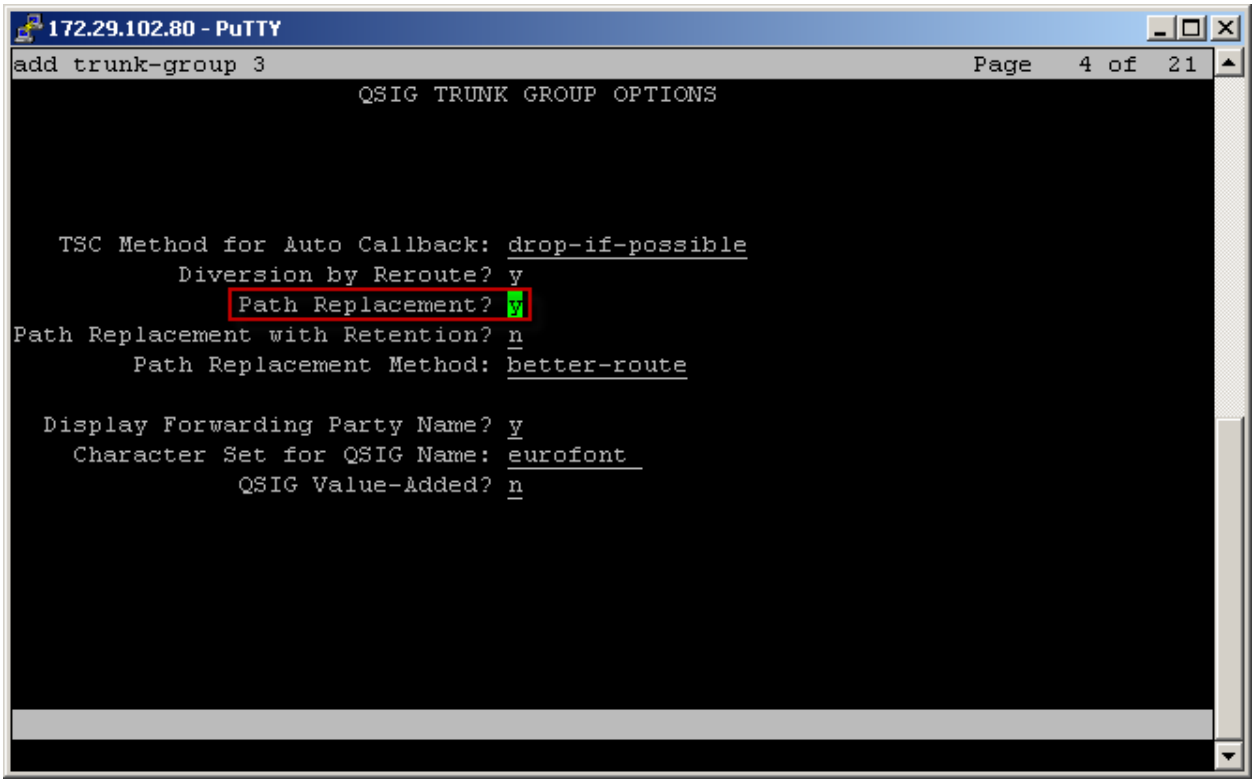

172.29.102.80 - PuTTY
add trunk-group 3 Page 2 of 21
Group Type: isdn
TRUNK PARAMETERS
Codeset to Send Display: 6 Codeset to Send National IEs: 6
Max Message Size to Send: 260 Charge Advice: none
Supplementary Service Protocol: b Digit Handling (in/out): enbloc/enbloc
Trunk Hunt: ascend
Digital Loss Group: 13
Incoming Calling Number - Delete: ___ Insert: Format:
Bit Rate: 1200 Synchronization: async Duplex: full
Disconnect Supervision - In? y Out? y
Answer Supervision Timeout: 0
Administer Timers? n CONNECT Reliable When Call Leaves ISDN? n
WARNING: Setting this field to "y" may result in trunk lock-ups

**5** On Page 3, set the following

| | |
|---|---|
| NCA-TSC Trunk Member | Set this to one of the Trunk Members |
| Send Name | y |
| Send Calling Number | y |
| Send Connected Number | y |

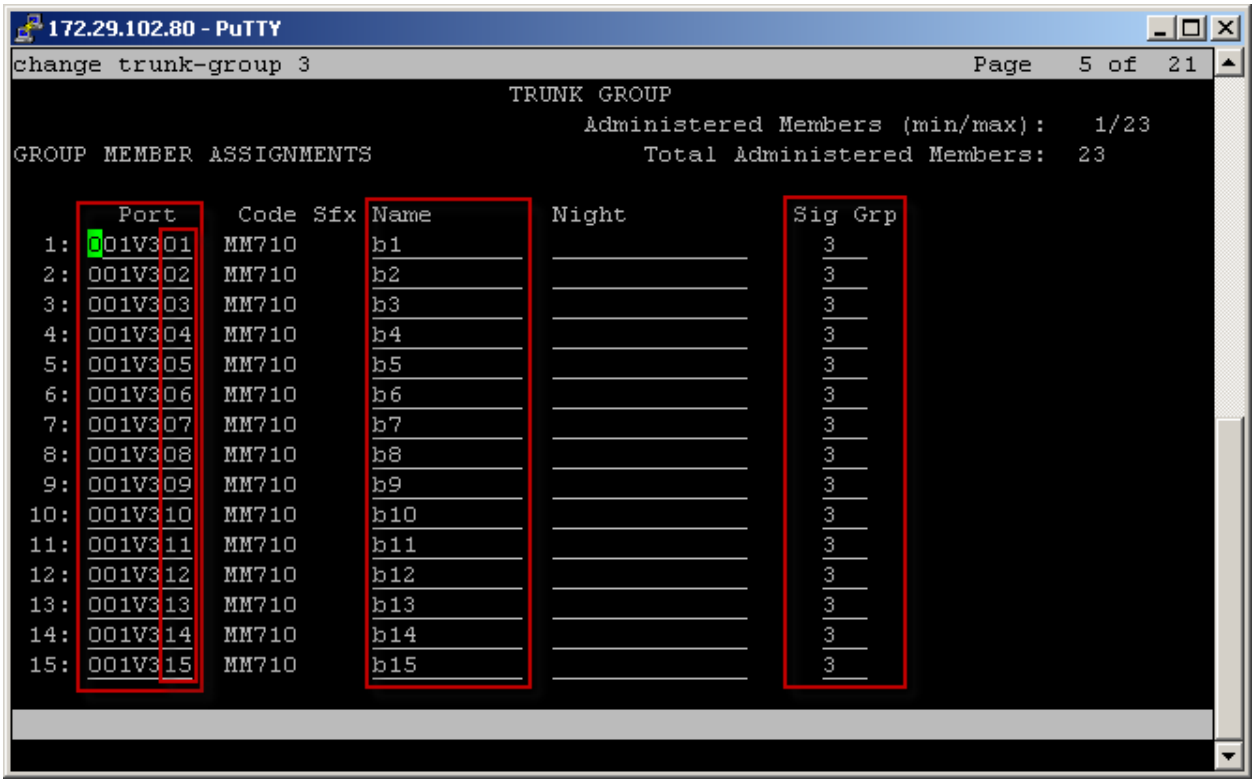

172.29.102.80 - PuTTY
add trunk-group 3 Page 3 of 21
TRUNK FEATURES
ACA Assignment? n Measured: none Wideband Support? n
Internal Alert? n Maintenance Tests? y
Data Restriction? n NCA-TSC Trunk Member: 3
Send Name: y Send Calling Number: y
Used for DCS? n Hop Dgt? n Send EMU Visitor CPN? n
Suppress # Outpulsing? n Format: public
Outgoing Channel ID Encoding: preferred UUI IE Treatment: service-provider
Replace Restricted Numbers? n
Replace Unavailable Numbers? n
Send Connected Number: y
Hold/Unhold Notifications? y
Send UUI IE? y Modify Tandem Calling Number? n
Send UCID? n
Send Codeset 6/7 LAI IE? y Ds1 Echo Cancellation? n
Apply Local Ringback? n
Show ANSWERED BY on Display? y
Network (Japan) Needs Connect Before Disconnect? n

**6** On page 4 ensure that Path Replacement is set to y


172.29.102.80 - PuTTY
add trunk-group 3
Page 4 of 21
QSIG TRUNK GROUP OPTIONS
TSC Method for Auto Callback: drop-if-possible
Diversion by Reroute? y
Path Replacement? y
Path Replacement with Retention? n
Path Replacement Method: better-route
Display Forwarding Party Name? y
Character Set for QSIG Name: eurofont
QSIG Value-Added? n

**7** On pages 5 and 6, enter the Individual trunks for channels 1-23.

| | |
|---|---|
| Port | The port number should correspond with the slot location you entered for the T1/ PRI, followed by the individual trunk number (1-23). |
| Code | This field should auto-populate with the media module type that is supporting the PRI. |
| Name | In this example, these were named b1 through b23. You can use whatever you'd like. |
| Signaling Group | Enter the Signaling Group number you created above. |



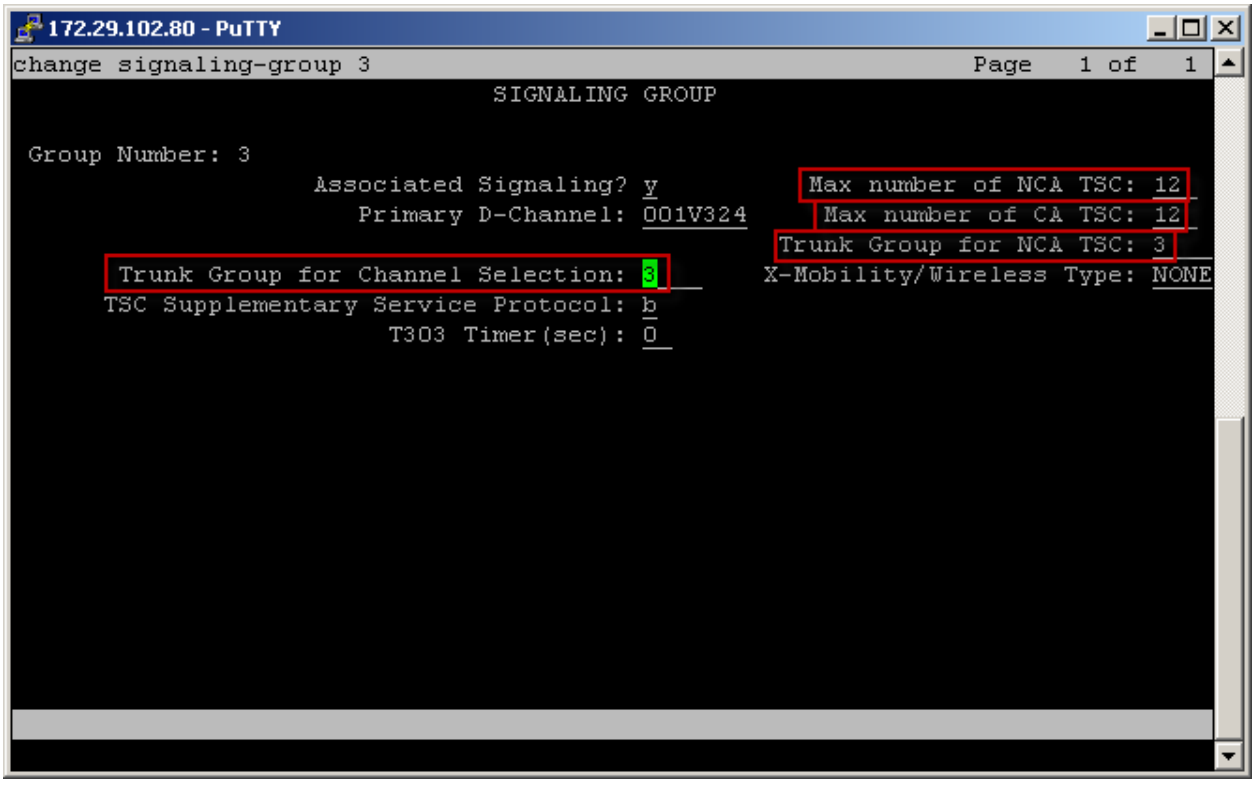

**8** Continue for all 23 ports.

## 4. Change Signaling Group

Now we must go back and change the signaling group. You might say "Why didn't we just add these fields to the signaling group when we created it?" Unfortunately, we have a bit of a chicken and egg problem. We can't select the trunk group for channel selection until we've created the trunk group, but we can't create the trunk group without specifying the signaling group that the trunk members will use.

1. Enter the command *change signaling-group x*, where x is the signaling group number you created above when you modified the signaling group.
2. Change the following fields:

| | |
|---|---|
| Trunk Group for Channel Selection | Enter the number of the trunk group configured in Step 3 |
| Max Number of NCA TSC: | 12 |
| Max Number of CA TSC | 12 |
| Trunk Group for NCA- TSC | Enter the number of the Trunk Group configured in Step 3. |

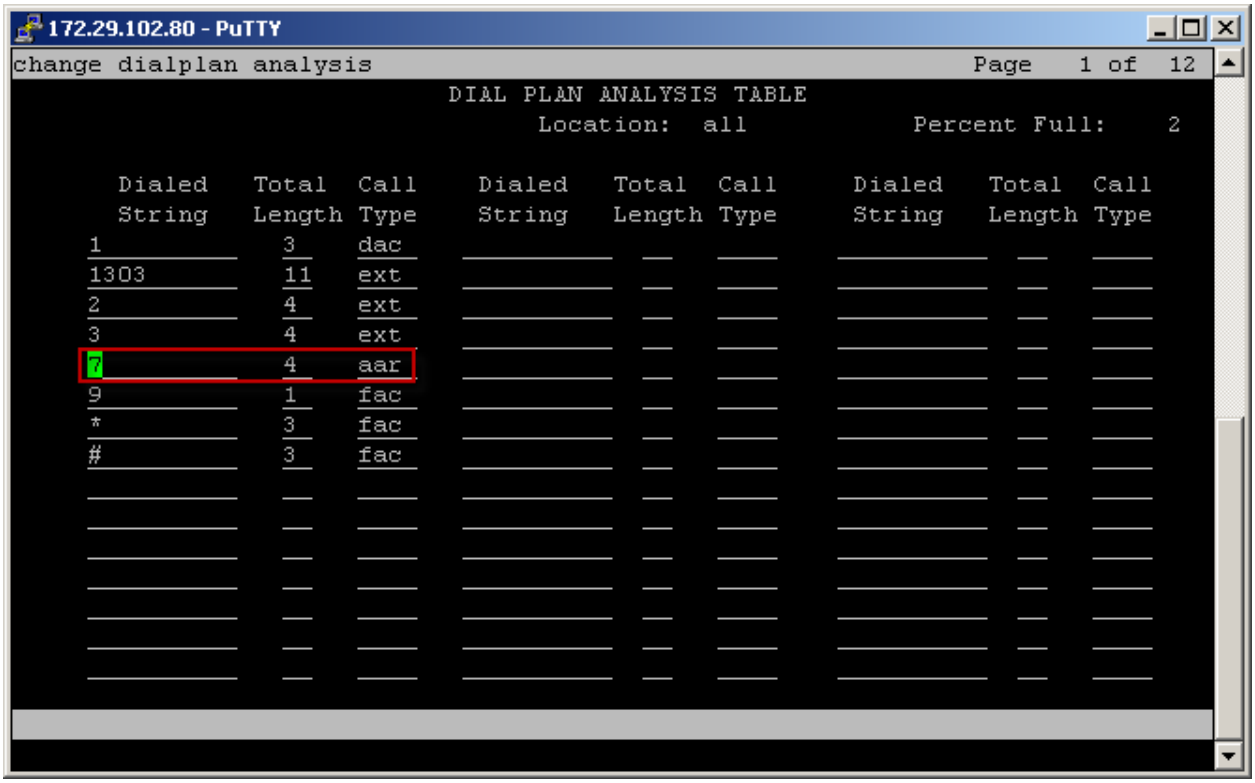

172.29.102.80 - PuTTY
change signaling-group 3
Page 1 of 1
SIGNALING GROUP
Group Number: 3
Associated Signaling? y
Primary D-Channel: 001V324
Max number of NCA TSC: 12
Max number of CA TSC: 12
Trunk Group for NCA TSC: 3
Trunk Group for Channel Selection: 3
X-Mobility/Wireless Type: NONE
TSC Supplementary Service Protocol: b
T303 Timer(sec): 0

## 5. Set up Dialing Parameters

Now we need a way to send calls intended for stations connected to the Mediant Gateway out the PRI. There are many ways to setup a dialplan in an Avaya system and detailing all of them is beyond the scope of this document. For our example we will assume that all calls intended for stations with a pattern of 70xx as their extension number will be sent out the PRI to the AudioCodes Mediant Gateway .

First, we need to ensure that the number range we wish to use is defined as a number we want the system to look at the aar analysis tables to decide how to route.

1. Enter the command change dialplan analysis.
2. For extensions with the format 7xxx, add a string to tell them to look at the aar table for information on which trunk group and route patterns to use to route the call.


172.29.102.80 - PuTTY
change dialplan analysis
Page 1 of 12
DIAL PLAN ANALYSIS TABLE
Location: all
Percent Full: 2
Dialed String | Total Length | Call Type
1 | 3 | dac
1303 | 11 | ext
2 | 4 | ext
3 | 4 | ext
7 | 4 | aar
9 | 1 | fac
* | 3 | fac
# | 3 | fac

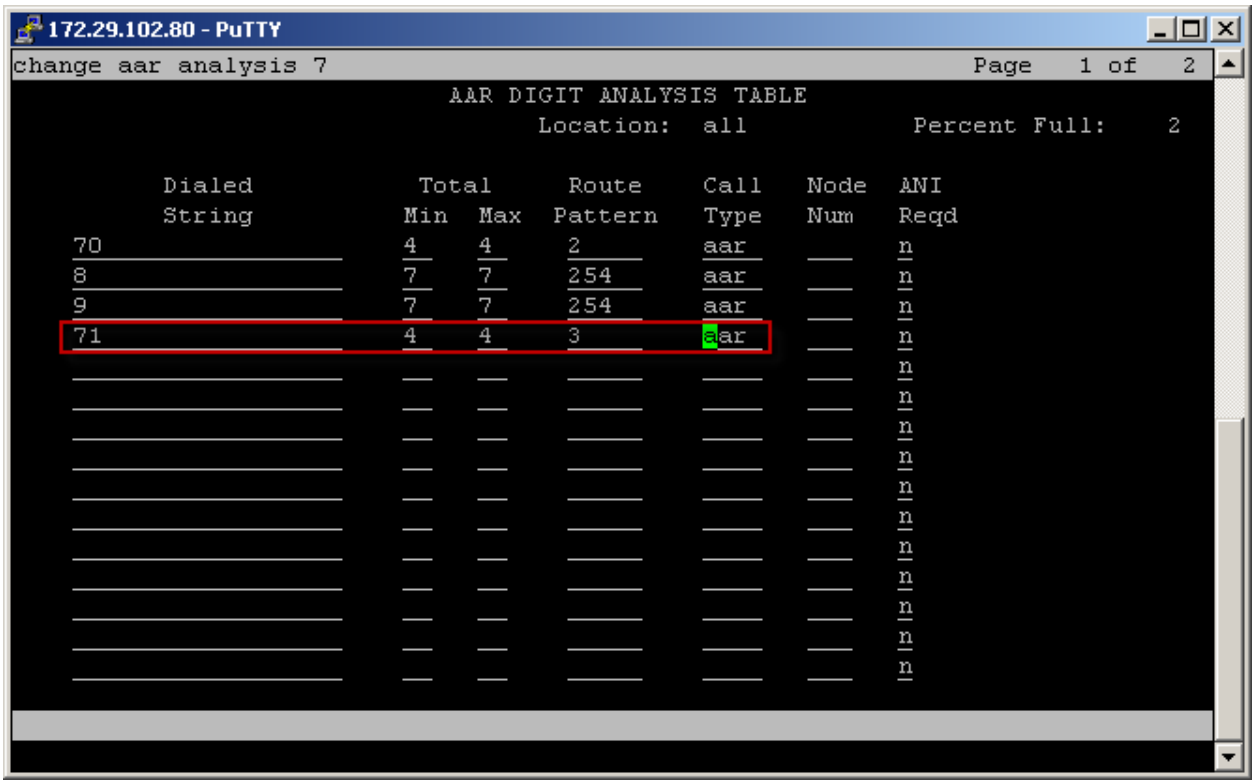
## 6. Change the Automatic Alternate Routing Table

Next we want to change the Automatic Alternate Routing table to tell the system that anytime someone dials 71xx, we want to send that call out the PRI to the second AudioCodes Mediant Gateway. You may need to add many entries to this table and the dialplan analysis table in order to accommodate your extensions.

**1** Enter the command *change aar analysis*.

**2** Add these parameters:

| | |
|---|---|
| Dialed String | Enter as much of the unique pattern as you can easily define This example is assuming that all extensions on the first gateway will be of the form 70xx, and all extensions on the second gateway will be of the form 71xx. |
| Total Min and Max | Enter the total number of digits in the extensions' length) |
| Route Pattern | Enter a unique number which will be used to create the route pattern in the next step. If you are unsure, cancel the current command and use the command *list route pattern.* Then define the next available number. |
| Call Type | aar |



## 7. Add the Route Pattern

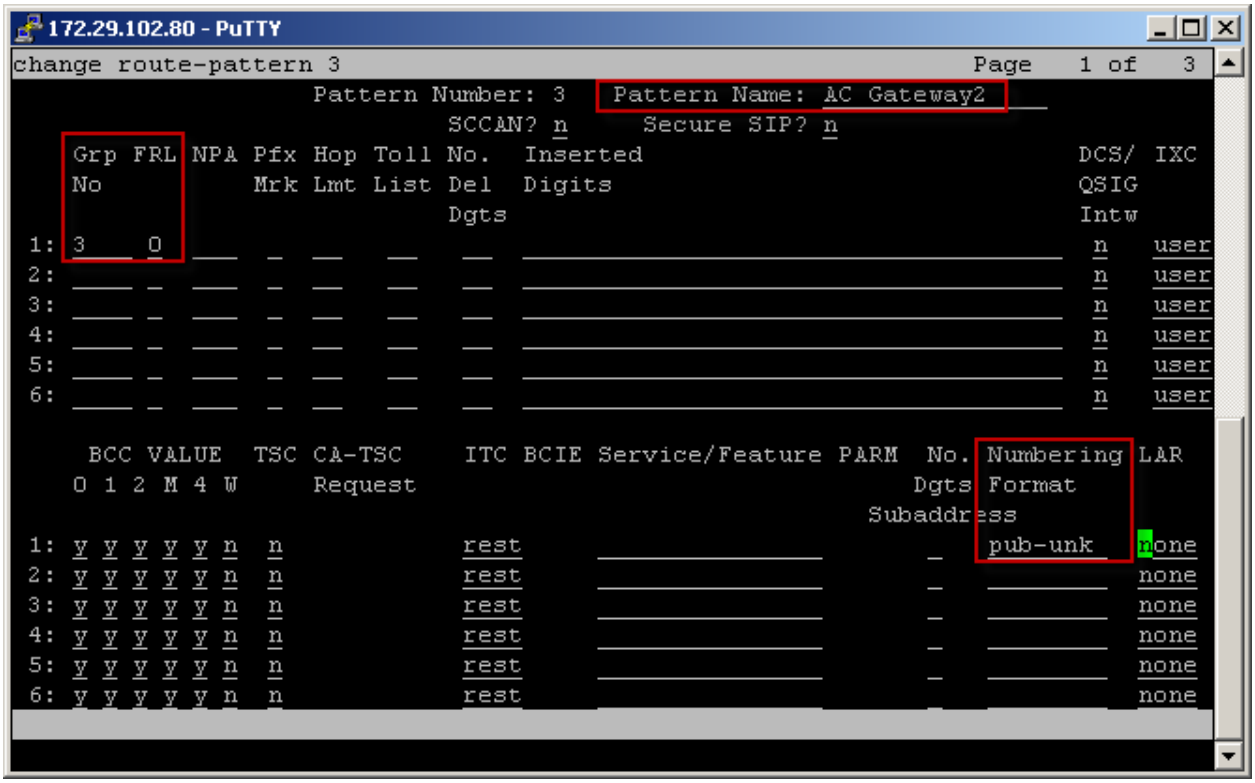
**Note: What are the existing route patterns?**

If some route patterns already exist in the system you would use the command *change route pattern x*.

**1** Enter the command *add route-pattern x*, where x is the number of the unique route pattern you created in step 7 (the test used 2).

**2** Set these parameters:

| | |
|---|---|
| Name | Enter a meaningful name. The test used AC_Mediant Gateway |
| Group Number | Enter the Trunk Group Number created in Step 3 (the test used #3) |
| FRL | Choose a facility restriction level that will not compromise your sites' security practices |
| Numbering Format | pub-unk |




**3** Press Esc-E to submit.

## 8. Set Caller ID

We also need to ensure we are sending the correct caller id. You can choose to send a full 10 digit caller ID, or send just the four digit caller id. For this example, we are sending the 4 digit caller id only.

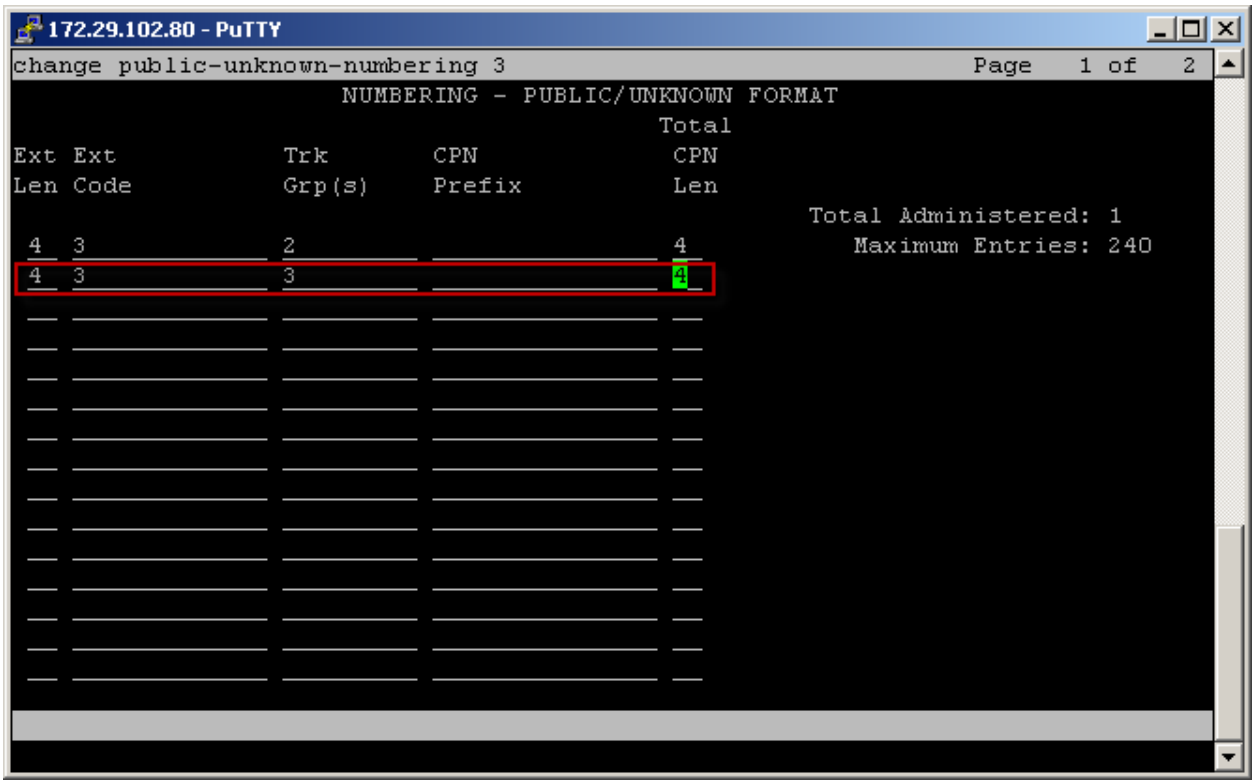
1 Use the command *change public-unknown-numbering.*

2 Set/change the following fields:

| | |
|---|---|
| Ext Length | 4 |
| Ext. Code | Enter the originating extension number range. In this case all CCMS phones were administered in the 3xxx range |
| Trk Grp | 3 |
| Total CPN Length | 4 |

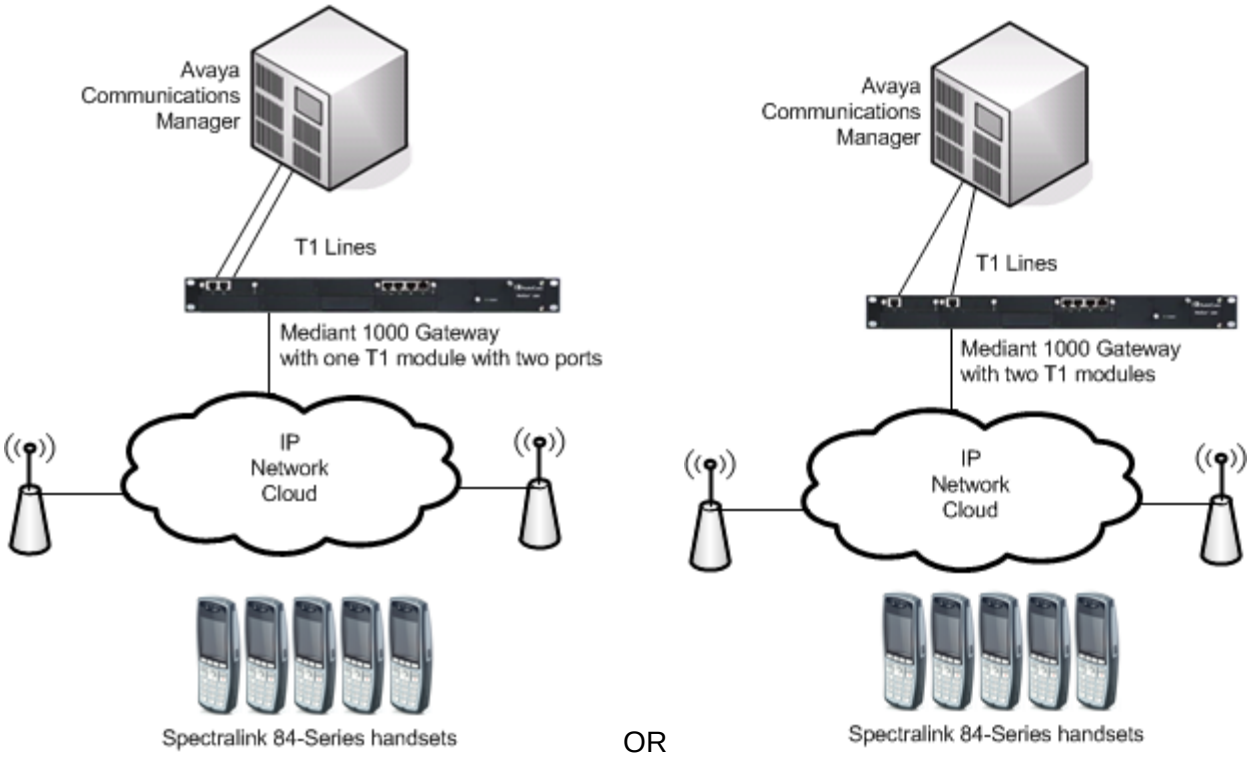
**Note: Specify Trunk Group**

We could specify both trunk Group 2 and 3 on the same line since we want the same behavior on both, but for example purposes, this one is built on a separate line.




## Adding a Second PRI to an Existing Trunk Group on the PBX

Another method of expansion is to add another trunk to the existing Mediant Gateway by either having a 2-port T1 module or adding a second T1 module. The PBX does not recognize the difference but the Mediant Gateway will need to be configured differently for each scenario.



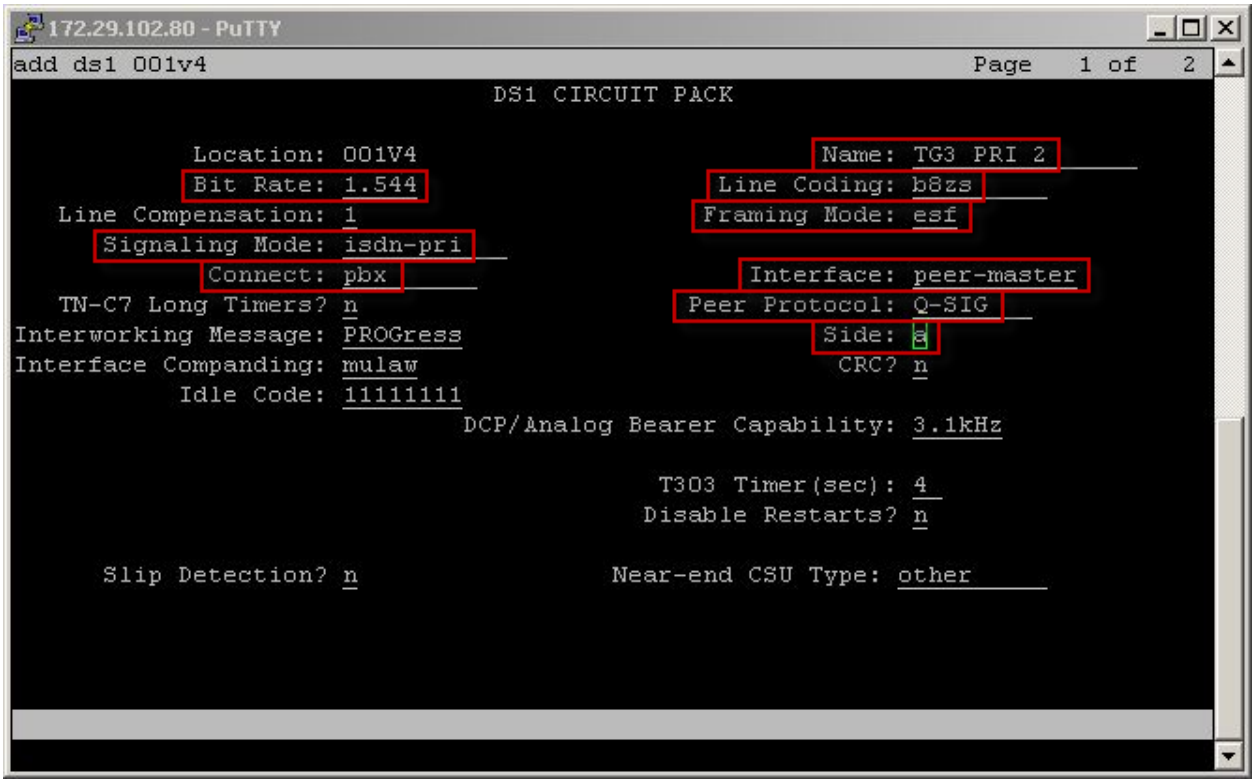

**Admin Tip: Allocate a second PRI card in the PBX**

You will need to install or allocate a second PRI card in the PBX for this configuration. We will add the trunks on this card to the same trunk group as one of our existing PRI's. (In this case TG #3) This will give us 23 additional channels in this trunk group. Note that we are using FAS (Facility Associated Signaling) for this integration and consider that this provides better service should a trunk failure occur.

## 1. Add the DS1

**1** Enter *add ds1 xxxxx command*, where xxxxx is the carrier/slot location of the DS1 connected to the Mediant 1000. For this configuration 001v4 was used. On page 1 of the ds1 form configure the following:

| | |
|---|---|
| Name | Enter something meaningful |
| Bit Rate | 1.544 |
| Line Coding | b8zs |
| Frame mode | esf |
| Signaling Mode | isdn-pri |
| Connect | PBX |
| Interface | peer-master |
| Peer Protocol | Q-SIG |
| Side | a |




**2** Press Esc-E to submit.

## 2. Add Signaling Group

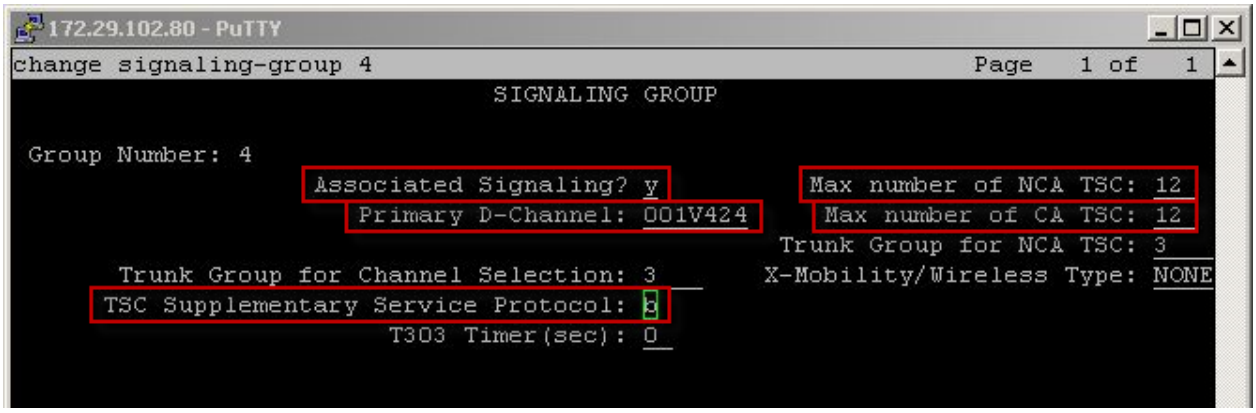
**1** Use the command *add signaling-group x*, where x is the number of the signaling group you wish to add.

**Note: What are the existing signaling groups?**

You can view the existing signaling-groups by executing a *list signaling-group* command.

**2** (Conditional) If you have a Group Type field, set it to isdn-pri. This field was not available in the 5.2 system but may be available on other system versions.

| | |
|---|---|
| Associated Signaling | y |
| Primary D Channel | Enter xxxxx24, where xxxxx is the location of the DS1 media module configured above. |
| TSC Supplementary Service Protocol | b |
| Max Number of NCA - TSC | 12 |
| Max Number of CA TSC | 12 |


172.29.102.80 - PuTTY
change signaling-group 4
Page 1 of 1
SIGNALING GROUP
Group Number: 4
Associated Signaling? y
Max number of NCA TSC: 12
Primary D-Channel: 001V424
Max number of CA TSC: 12
Trunk Group for NCA TSC: 3
Trunk Group for Channel Selection: 3
X-Mobility/Wireless Type: NONE
TSC Supplementary Service Protocol: b
T303 Timer(sec): 0

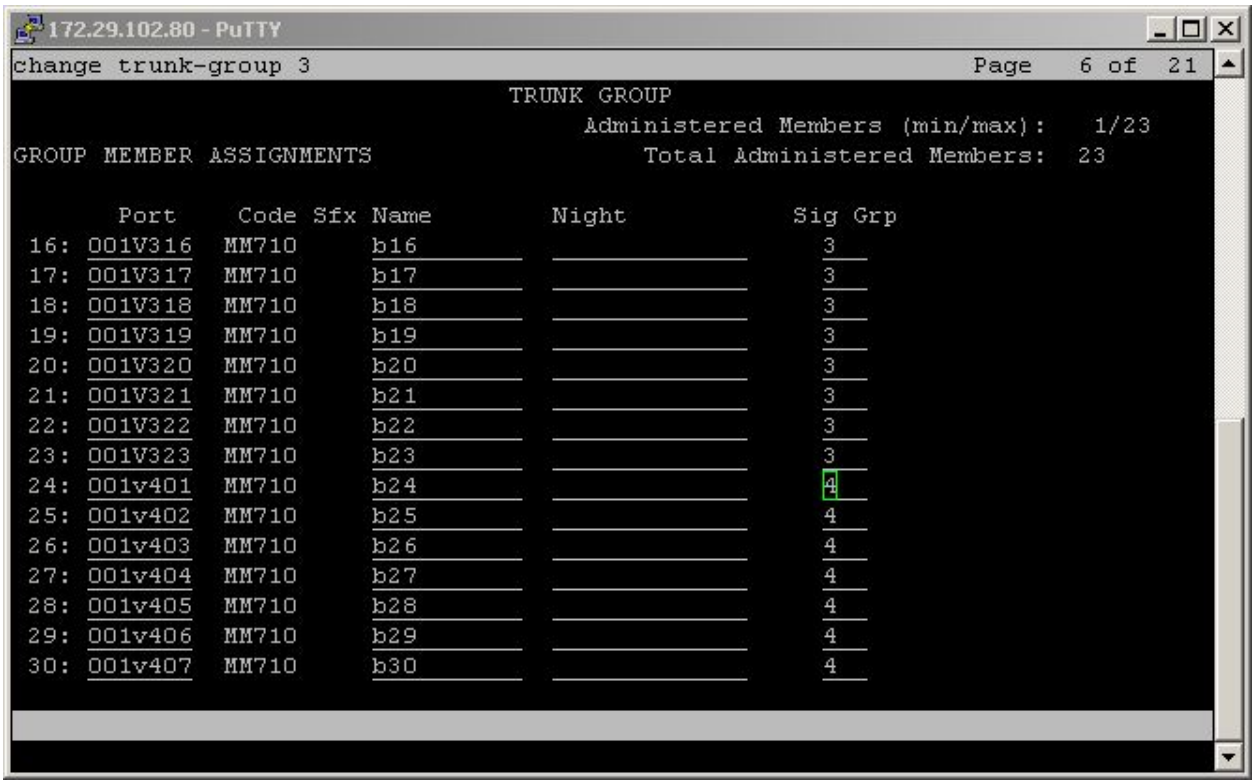
**3** Press Esc-E to submit.

### 3. Add Channels

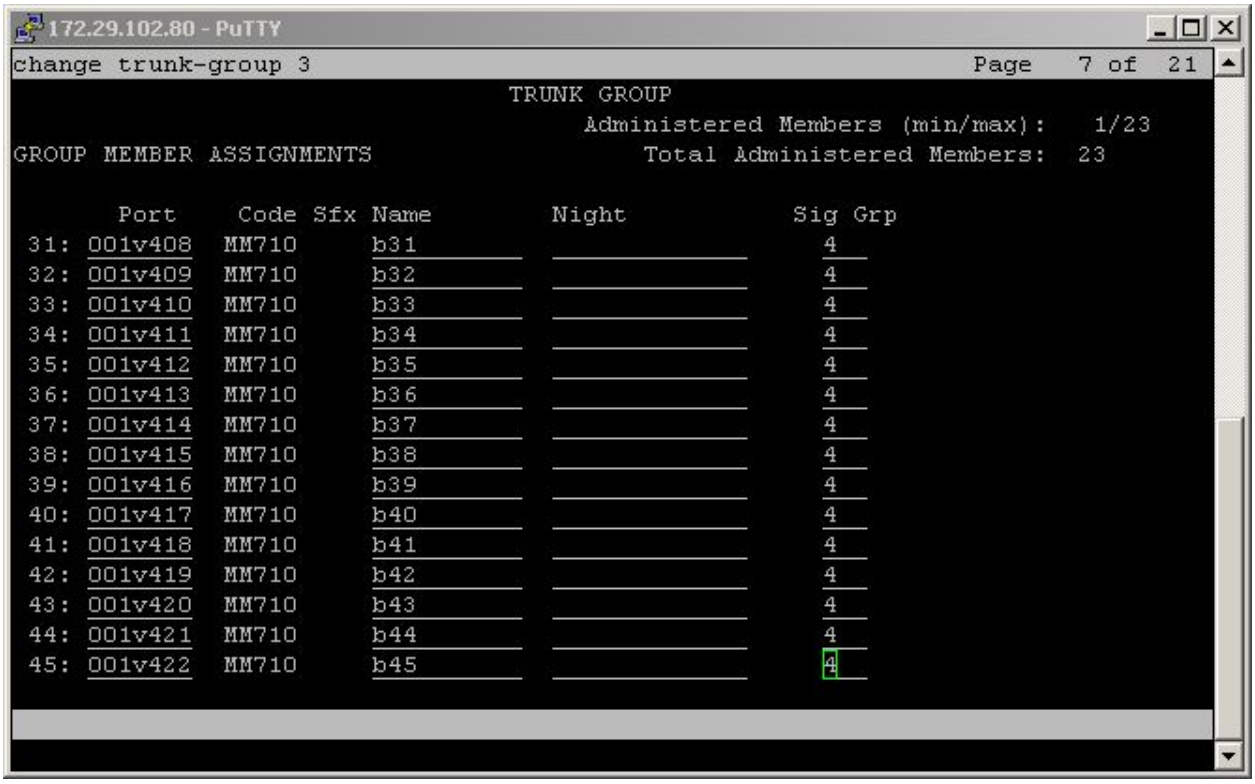
The next step is to add the channels of the newly created PRI to the Already Existing Trunk Group (In my example this is TG #3).

**1** Enter the command *change trunk-group 3.*

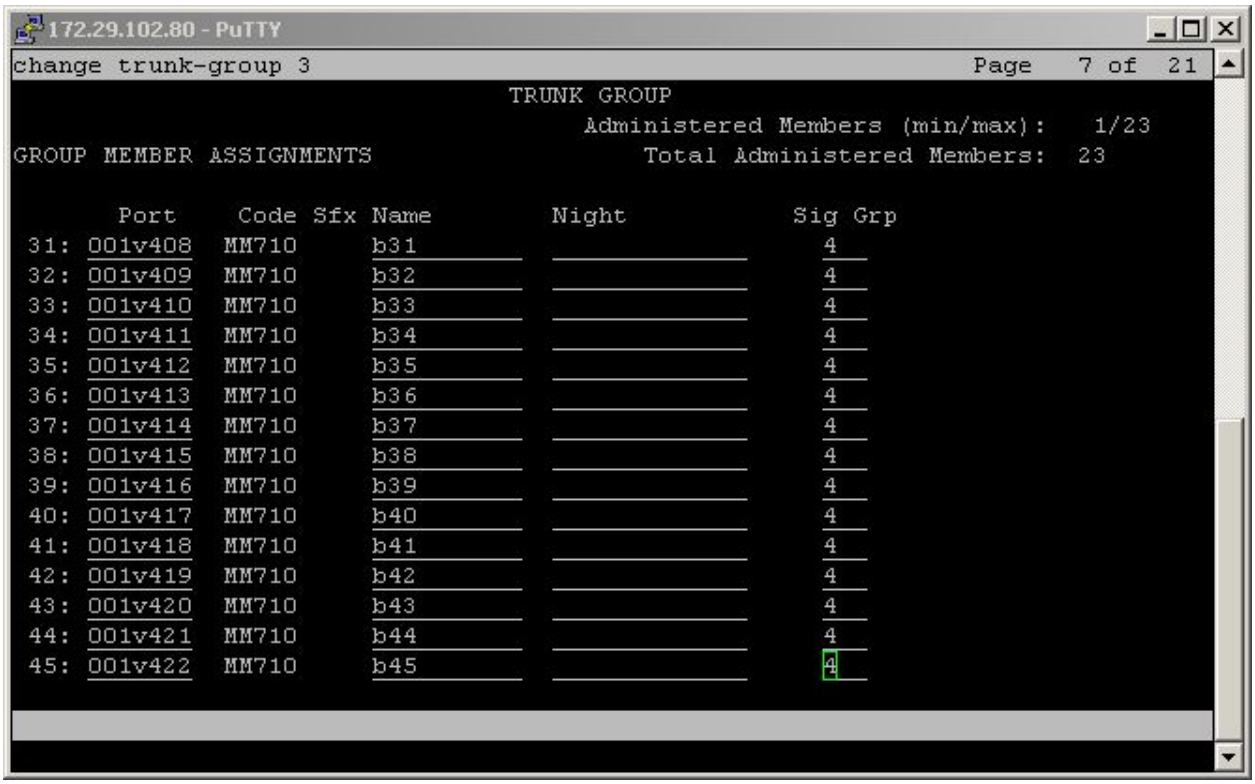
**2** Navigate to the Trunk Group Member page and begin adding your trunks. In this case the second PRI's trunks were added on page 6 and 7 of the trunk group form.



**3** Continue to the next page.




**4** And the last trunk on the next page…



## 4. Configure the AudioCodes Mediant Gateway

On the Mediant Gateway side there are two possibilities; the first is that we have a single T1 module with two PRI interfaces in it, and the second is that we have two separate T1 modules each with a single PRI interface. Trunk Group settings need to be changed depending on which system you are using.

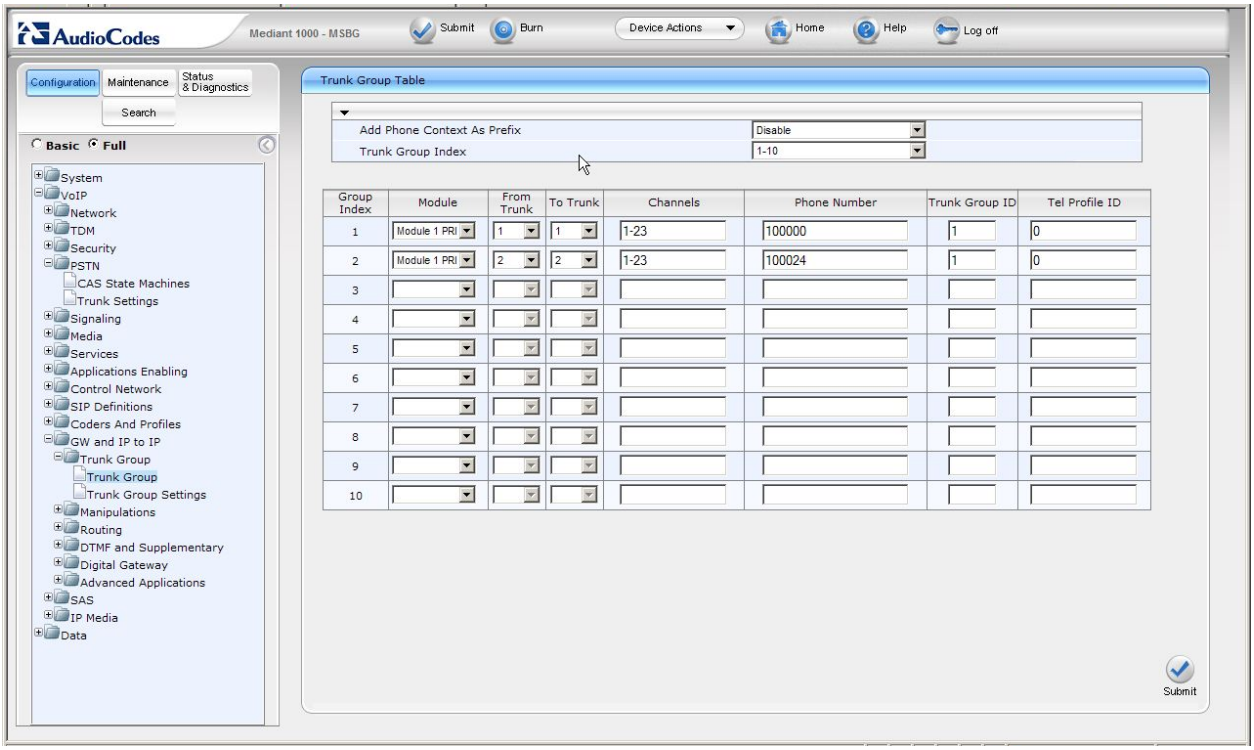
### a. Change the Trunk Group settings

*Two PRI interfaces in one T1 module*

**1** Select the Configuration tab and navigate to VOIP > GW and IP to IP > Trunk Group > Trunk Group.

**2** Change these settings:

| | |
|---|---|
| Module | Select the module for the second PRI (The same module as the first PRI) |
| From Trunk | 2 |
| To Trunk | 2 |
| Channels | 1-23 |
| Phone Number | 100024 (Begin with the next available channel number) |
| Trunk Group ID | 1 |
| Tel Profile ID | 0 |



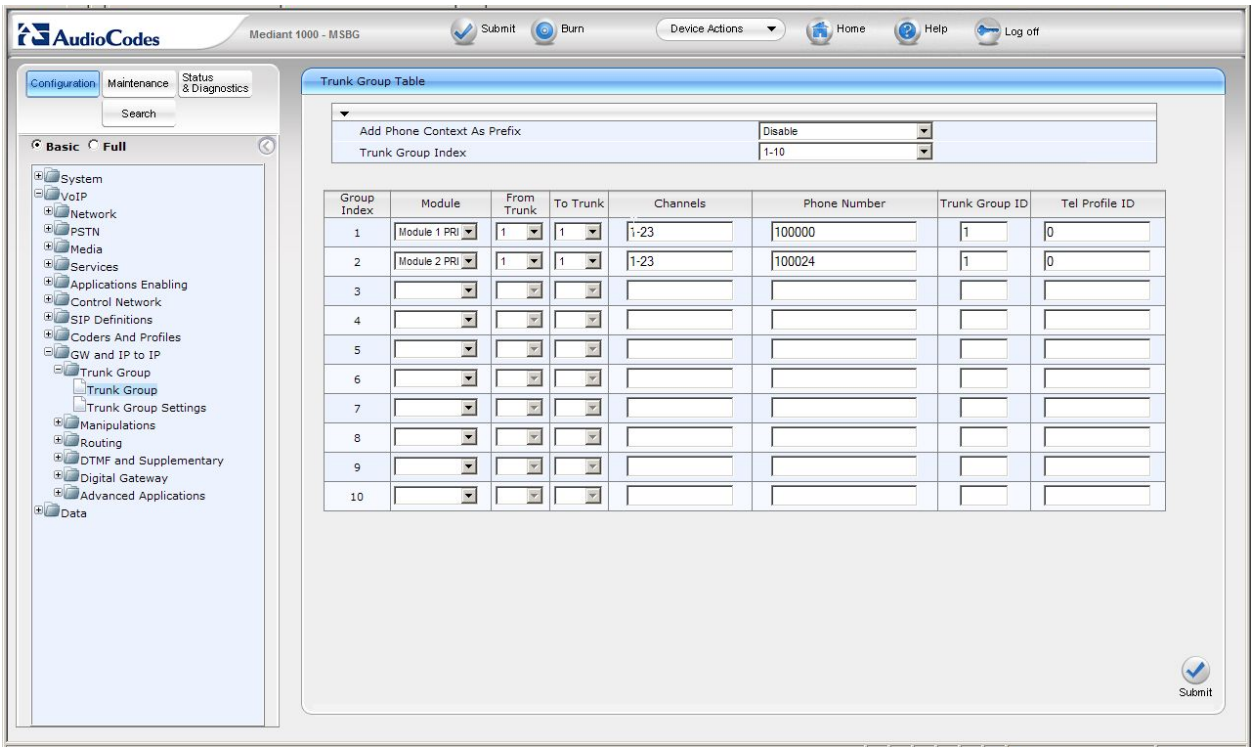

**3** Press **Submit** and **Burn**.

*Two PRI interfaces in two T1 modules*

**1** Select the Configuration tab and navigate to VOIP > GW and IP to IP > Trunk Group > Trunk Group.

**2** Change these settings:

| | |
|---|---|
| Module | Select the module for the second PRI |
| From Trunk | 1 |
| To Trunk | 1 |
| Channels | 1-23 |
| Phone Number | 100024 (Begin with the next available channel number) |
| Trunk Group ID | 1 |
| Tel Profile ID | 0 |

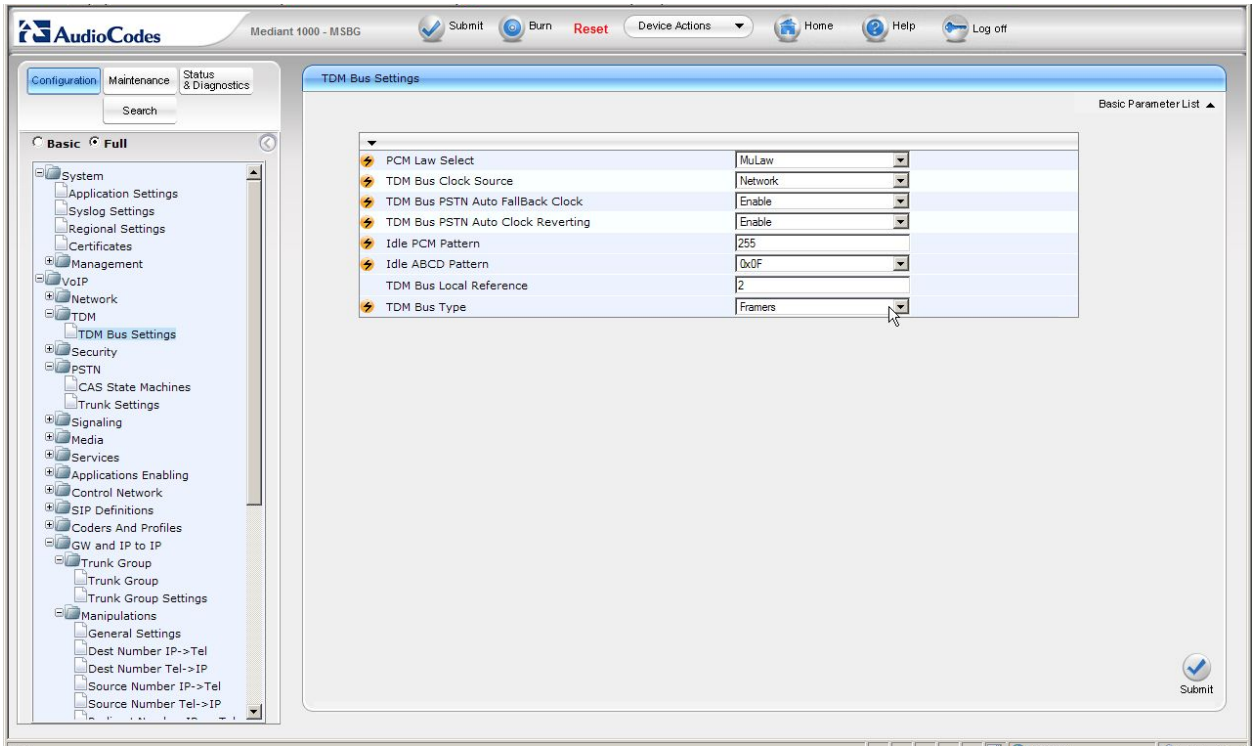



**3** Press the **Submit** button and **Burn**.

## b. Add Second PRI as Clock Source

When using Multiple PRI's we will also want to allow the PRI to use the secondary PRI as a clock source. With this configured, if the first PRI becomes out of service for some reason, the Mediant Gateway can use the second PRI for clocking.

1. Select the Configuration tab and navigate to VOIP > TDM > TDM Bus Settings.
2. Enable TDM Bus PSTN Auto Fallback Clock
3. Enable TDM Bus PSTN Auto Clock Reverting




4. Press **Submit** and **Burn**.

## c. Modify PSTN Trunk Settings

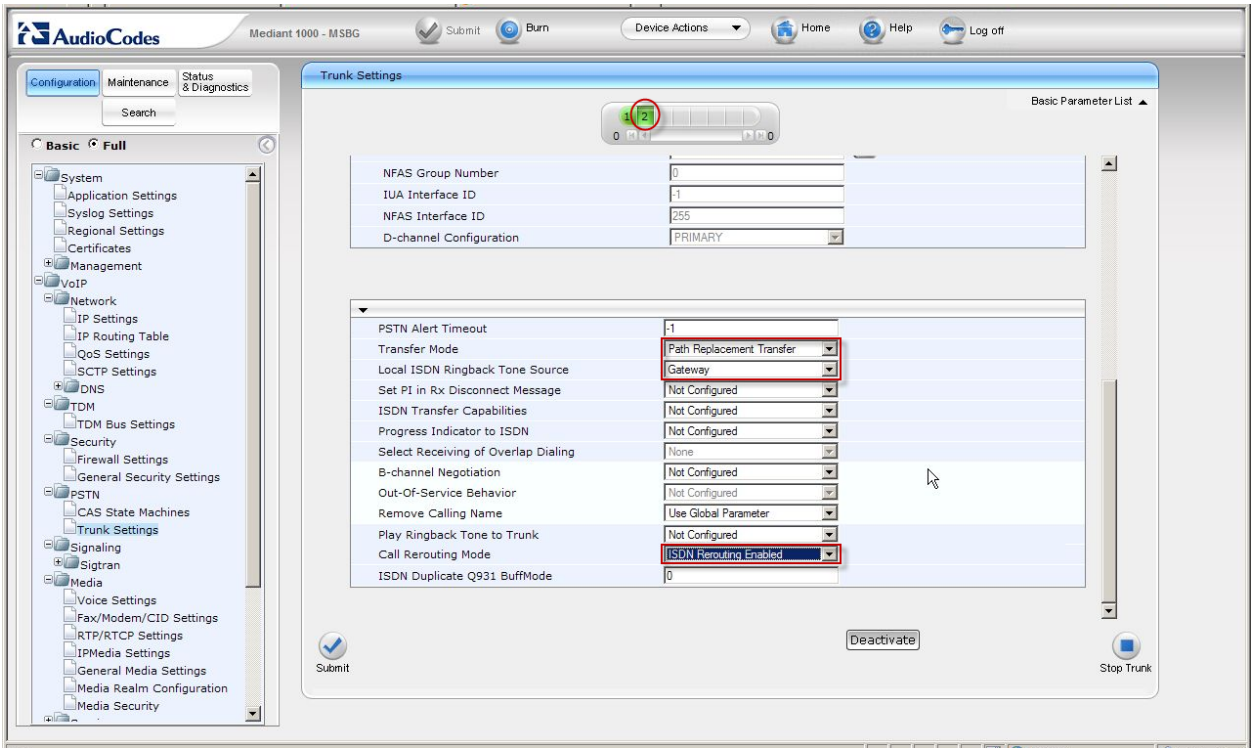
The Trunk Settings for the second PRI need to be modified. Navigate to VoIP => PSTN => Trunk Settings, and click on the 2nd trunk at the top of the screen. (This will apply regardless of whether the additional trunks are in the same module or two separate modules). We now need to configure the same settings that we applied to the first trunk

**1** Select the Configuration tab and navigate to VOIP > PSTN > Trunk Settings.

**2** Click the second trunk at the top of the screen.

**3** Modify these parameters:

| | |
|---|---|
| Transfer Mode | Path Replacement Transfer |
| Local ISDN Tone Ringback Source | Mediant Gateway |
| Call Rerouting Mode | ISDN Rerouting Enabled |




**4** Press **Submit** and **Burn**. Reboot the Mediant Gateway .

# Part III: Deployment, Testing and Troubleshooting

Part III covers the deployment of the solution in a functional environment and adjusting the configuration to provide specific functionality for certain features, as needed. Testing features and resetting the Mediant Gateway are also covered here.

# Chapter 11: Testing Mediant Gateway to PBX Functionality

| | |
|---|---|
| Outgoing Call to PBX Station | From an 84-Series handset registered to the Mediant Gateway , dial a station attached directly to the PBX. Ensure the calling party hears ringback and the called party's phone rings. Answer the call and verify two way voice path. Check that the Caller ID is also appropriate. |
| Incoming Call from the PBX | From a station attached to the PBX, dial an 84-Series handset. Ensure the calling party hears ringback and the called party's phone rings. Answer the call and verify two way voice path. Check that the Caller ID is also appropriate. |
| Transferring a call from a PBX Station to the 84-Series handset | From an 84-Series handset registered to the Mediant Gateway , dial a station attached directly to the PBX. Answer the call and initiate a transfer to another 84-Series handset. Verify you can successfully transfer the call. |
| Outgoing Call to the PSTN | From an 84-Series handset registered to the Mediant Gateway , dial a PSTN number (such as your cell phone). Remember to include the ARS code necessary to reach an outside line from the PBX just as you would from a station directly attached to the PBX. Verify the PSTN number rings and can be answered with two way voice path. Check Caller ID on both the 84-Series handset and the PSTN phone.<br>If you register the 84-Series handsets as 4 digit extension numbers, and then place calls to the PSTN, the PBX will simply pass our 4 digit caller id from the 84-Series handsets to the PSTN if Send Calling Number is configured on the PSTN Trunk Group in the Avaya PBX. The PSTN is likely to insert the Trunks' Billed Telephone Number into this field as a response to what it perceives as an "invalid" Caller ID. In this case the caller's actual DID number will not be presented. Please refer to Program a 10-digit Caller ID in Chapter 12 for a suggestion of one way to resolve this issue. |
| Call Hold & Resume | From an 84-Series handset registered to the Mediant Gateway , dial a station attached directly to the PBX. Answer the call and initiate a hold from the 84-Series handset to the PBX station. The held party will not hear any Music on Hold or Comfort Tone. Retrieve the call using the Resume softkey.<br>Next place the 84-Series handset on hold from the PBX station and then resume the call. The held party will hear Music On Hold if supplied by the PBX. |

# Chapter 12: Troubleshooting

## Features

### Transfer

If you are just transferring between extensions attached to the AudioCodes Mediant Gateway , then the PBX's configuration shouldn't matter, but if you are transferring to and from extensions attached to the PBX, the PSTN, or another Mediant Gateway then the PBX's settings are very important. Here are a few things to check if these types of transfers (or conferences) are not working:

1. (ACM) On Page 2 of the trunk group form, ensure Disconnect Supervision is set to a value of Y for both In and Out
2. (ACM) Check Page 1 of the *change system-parameters features* form. You may want to try setting the Trunk-to-Trunk transfer field to a value of **all**.

**Caution: Toll fraud warning**

This configuration will increase your system’s exposure to toll fraud.

### Call Forward

If users want to be able to Call Forward from extensions on the PBX to mobile extensions you need to set the Class of Service of the phone that is doing the forwarding to a COS that does not Restrict Call Fwd-Off Net

1. (ACM) Check parameters:
    - Check the current COS of the station by doing a *display station xxxx* command (where xxxx is the stations' extension number). The COS will be one of the fields on the first page, in the upper right hand corner
        - Ensure with the customer that it is ok if all stations with this COS be modified to allow call forward off net if this field needs to be toggled; if not they may need to create a new COS for specific phones that will require this ability. (For some customers this may be a toll fraud concern.)
    - Check the COS's restriction level by using the change cos command. Your stations COS is listed in the top row Look vertically down beneath your stations COS for the field *Restrict Call Fwd-Off Net.*
        - If this is currently set to a value of Y, this is at least part of the reason why Call Forward to the 84-Series handset is not working for you. Change it to a value of n

2. (ACM) Change value
    - You may also need to change the value of *the Threshold for Blocking Off-Net Redirection of Incoming Trunk Calls* to a value of n. You can find this parameter on page 1 of the *change system-parameters coverage-forwarding form.*

## Caller ID

There are many ways to handle Caller ID in the Avaya PBX. This document details a way we found to work in our testing lab. If you are experiencing issues with caller ID not being delivered from the Avaya system to the 84-Series handset Mediant Gateway , or the PSTN, below are a few of the places you might look first.

If you are not receiving Caller ID from an Avaya station when calling an 84-Series handset connected to an AudioCodes Mediant Gateway :

1. (ACM) Check Page 2 of the calling station's form using the *change station xxxx* command. Look for the field "Per Station CPN - Send Calling Number" - Ensure this is set to a value of Y
2. (ACM) Check the *change public-unknown-numbering x* form. Recall that you will want to specify what number (and prefix) are sent out to various trunk groups. When sending to another Mediant Gateway , you will probably want to just send the extension number, but if you are sending calls to the PSTN, you will probably want to include the full ten digit number.
3. (ACM) If you are trying to send the calling party name out a NI2 trunk check the *change system-parameters features* form and ensure that the variable *USNI Calling Name for Outgoing Calls* is set to a value of Y

### Program a 10-digit Caller ID

In some cases, you may wish to modify the Caller ID that you are sending. In the examples used in this application note, we were sending a four digit Caller ID because that is how we registered the phones to the Mediant Gateway Mediant Gateway , as four digit extensions. This worked well when communicating with other extensions on the PBX, or extensions on another Mediant1000 Mediant Gateway attached to the PBX. However, when you begin calling to other off-PBX locations, a four digit Caller ID may not be appropriate. Consider the case where you wish to send an entire 10 digit Caller ID, such as when you are planning on placing calls out to the PSTN. For on-PBX stations in the ACM you would normally modify your Caller ID using the *change public-unknown-numbering* command. In the example below we show you where you would go to modify your outbound Caller ID for stations registered to the Mediant 1000.

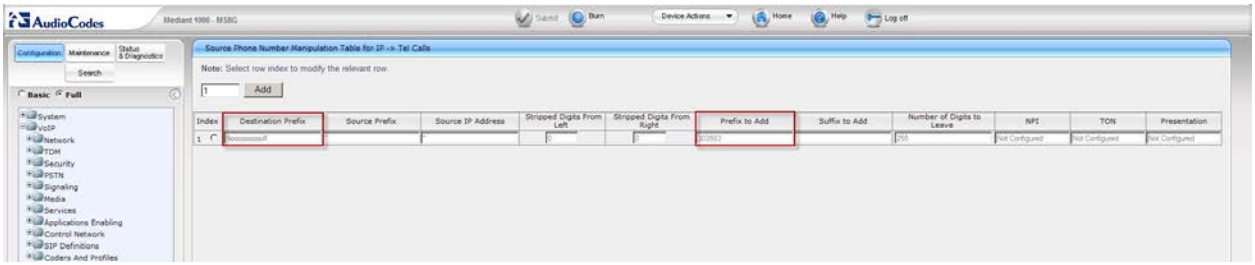
1. (AUDC) Navigate to VOIP->GW and IP to IP->Manipulation->Source Number IP->Tel

    In our example below, all of our DID numbers registered to the ACM begin with 303-583, followed by the number we used for registration. Our Avaya ACM is also configured to use 9 as the ARS Access-Code 1.

2 Configure:

**c** Destination prefix = 9*

**d** Prefix to Add = 303583 (adds a 6 digit prefix to the existing 4 digit extension of the phone)




3 **Submit** and **Burn**.

# Resetting the Mediant Gateway

## Clearing the configuration

### Manual method

If you have a situation where the box completely freezes, you can reset it to factory defaults by inserting a paperclip in the tiny hole on the CPU board. Hold it in for about 6 seconds until the LAN LED starts blinking and then release the clip. The box will reboot and search for a new ini file.

### Software method

You may also reset the Mediant Gateway's configuration by loading an empty board.ini file, using the Web interface. The only settings that are not restored to default using this method are the management (OAMP) LAN IP address, the Default Gateway address, and the Web interface's login user name and password.

**How to prepare an empty .ini file:**

The ini file to be loaded must be empty (i.e., contain no parameters) or include comment signs (i.e., semicolons ";") preceding lines (parameters). One method to create this file:

1 Open a new notepad doc, do not type anything into it as text.

2 Save the document, naming it **empty.ini**. The result should be a 0kb file named empty.ini

**To restore defaults using the Web interface:**

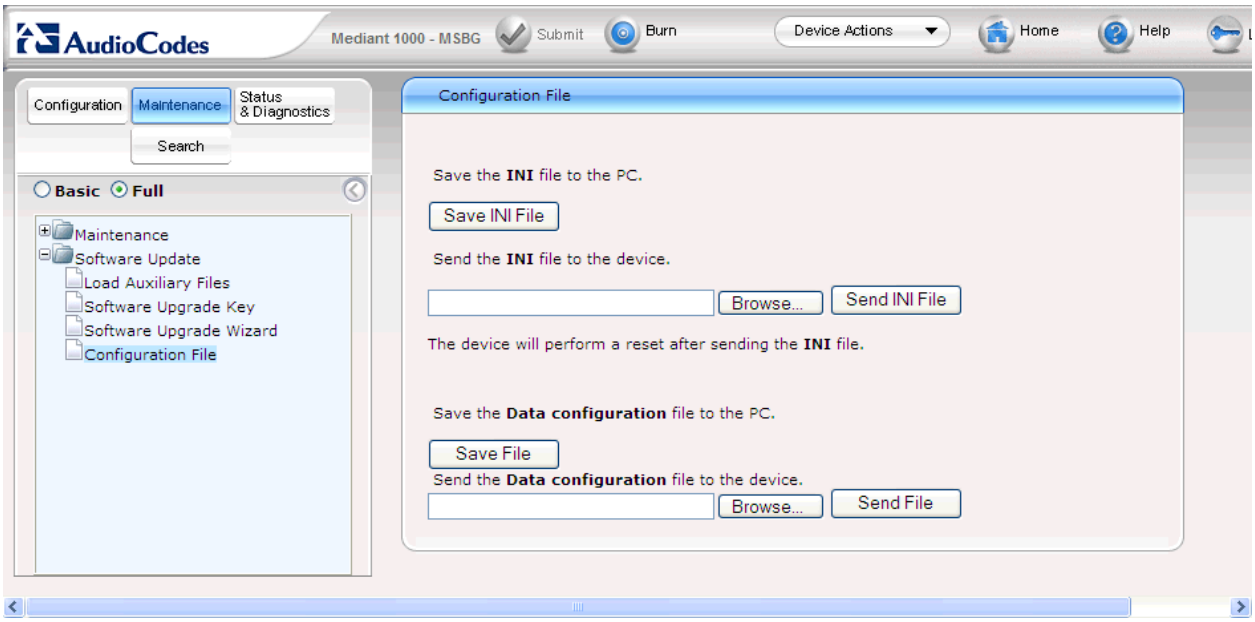
1 Prepare an empty ini file (empty.ini) and save it in a folder on your PC.

2 Log on to the Web interface.

3 Open the Configuration File by doing one of the following:

**a** On the toolbar, click Device Actions, and then choose Load Configuration File. Or,

**b** Open the Maintenance tab and navigate to Software Update > Configuration File.




4 Click the Browse button corresponding to the Send INI File button, navigate to the empty ini file, select the file, and then click Open.

5 Click the Send INI File button, and then at the prompt, click OK; the device uploads the ini file and then resets the device to default settings (based on the cmp file currently running on the device).

6 After a few minutes you should be able to browse back into the device using the same IP address the device had prior to restoring defaults.

## Using the serial adapter cable

(see AudioCodes document LTRT-30300 *Restoring Factory Defaults Technical Note*)

A serial adapter cable ships with the Mediant Gateway and it is used when you cannot access the Mediant Gateway through the network. It has a proprietary com port connector which is not commercially available through other sources. Please keep this cable close to the Mediant Gateway in case troubleshooting is needed.

# Part IV: Appendices

Part IV contains Appendices: Module Maintenance, Software Upgrade Procedure and a sample .ini file are included.

# Appendix A: Module Maintenance

The T1 module can be removed or added while the GW is operational but will not be activated until the Mediant Gateway is rebooted.

On the home screen, select the module by pointing to the slot title “Digital” and double click. A popup “Remove Module” will appear. Click and follow the instructions.

**Caution**

If you only have one T1 card, you will get an error message as removing the card will make the Mediant Gateway inoperable and calls will be terminated/not allowed. If you need redundancy, you will need two T1 cards.

Once the removal is done, the slot title will display Digital Reserved.

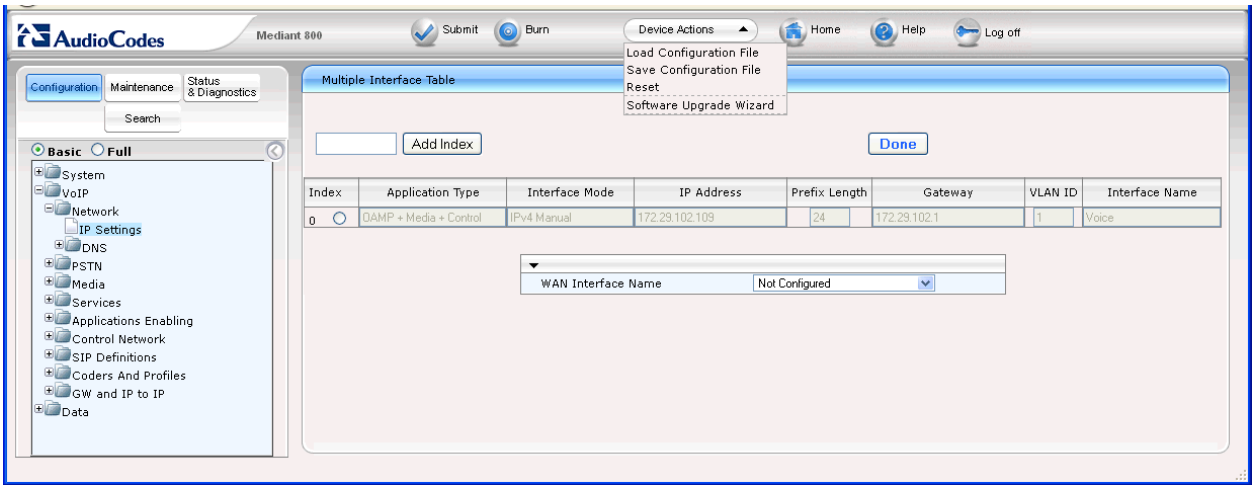
To insert the new module, double click the slot title and insert the new module. The module will be recognized. You may have to reboot the Mediant Gateway in order for the module to activate.

# Appendix B: Software Upgrade Procedure

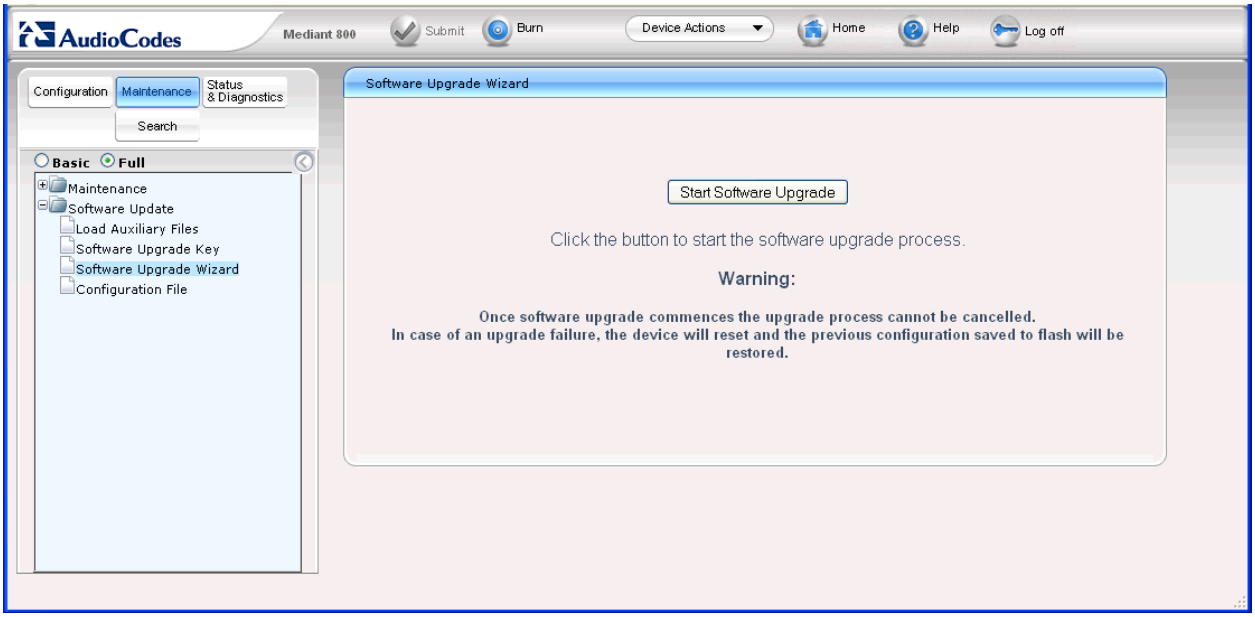
When you need to upgrade the software, follow this procedure:

Obtain the software from your service representative. It will be a .cmp file. Download or copy it to a location where you can retrieve it.

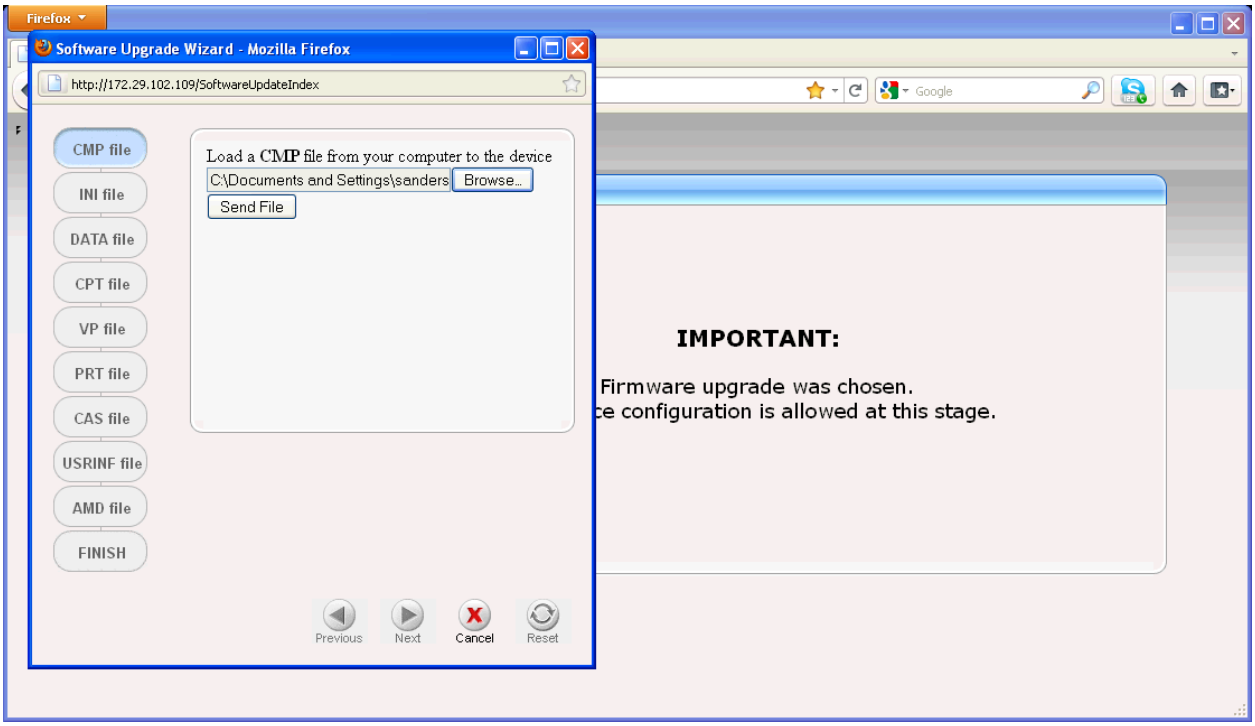
Use Device Actions and select Software Upgrade Wizard to open the wizard.



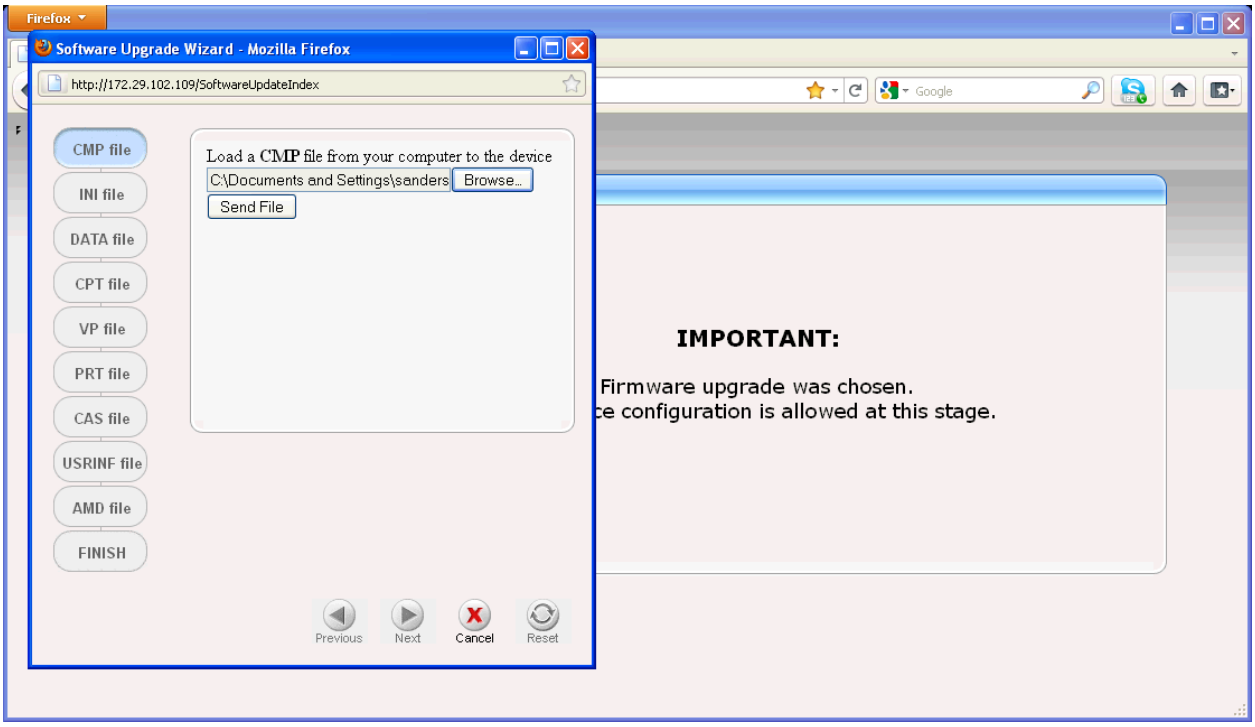

Click Start Software Upgrade.



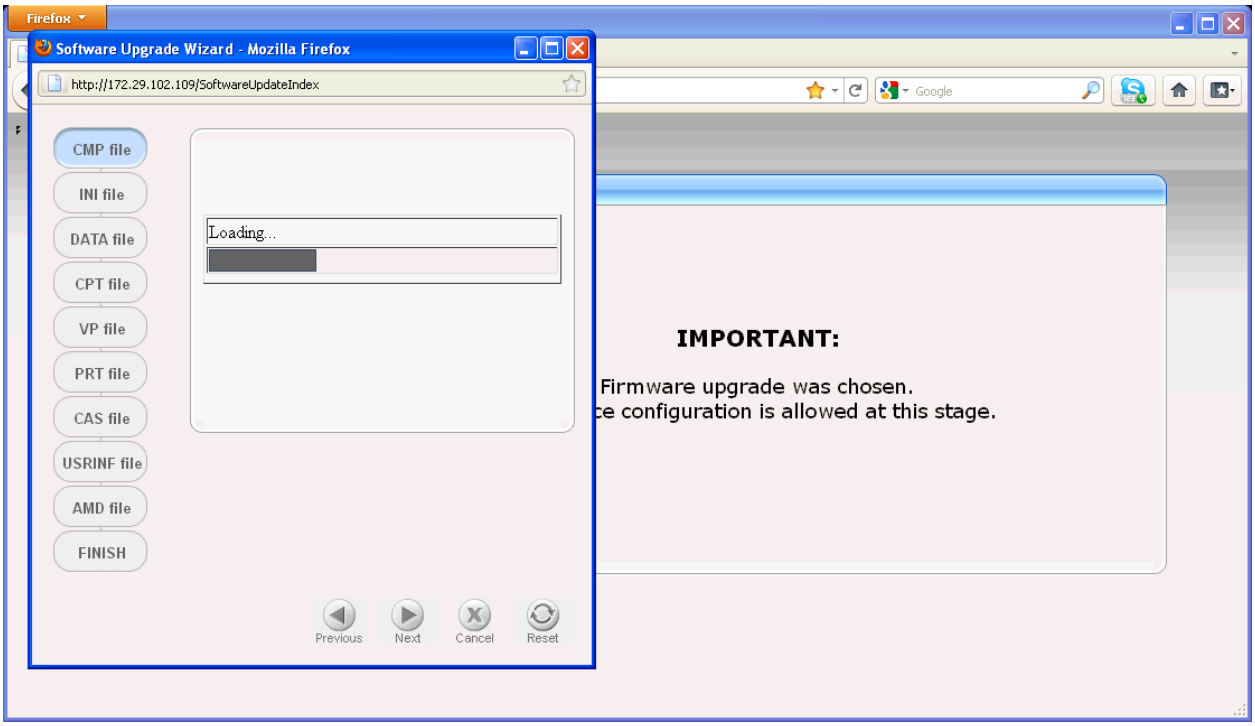

You will be prompted for the .cmp file. Browse to the location and click the file.



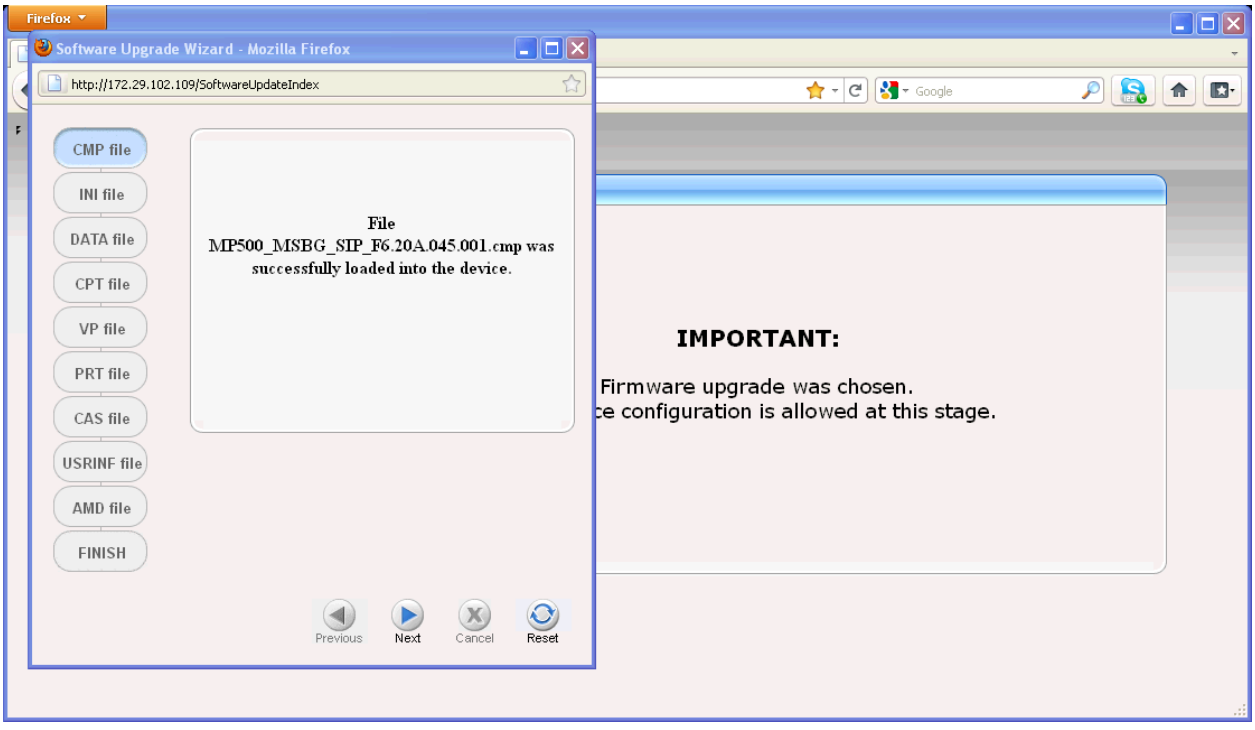

press Send file



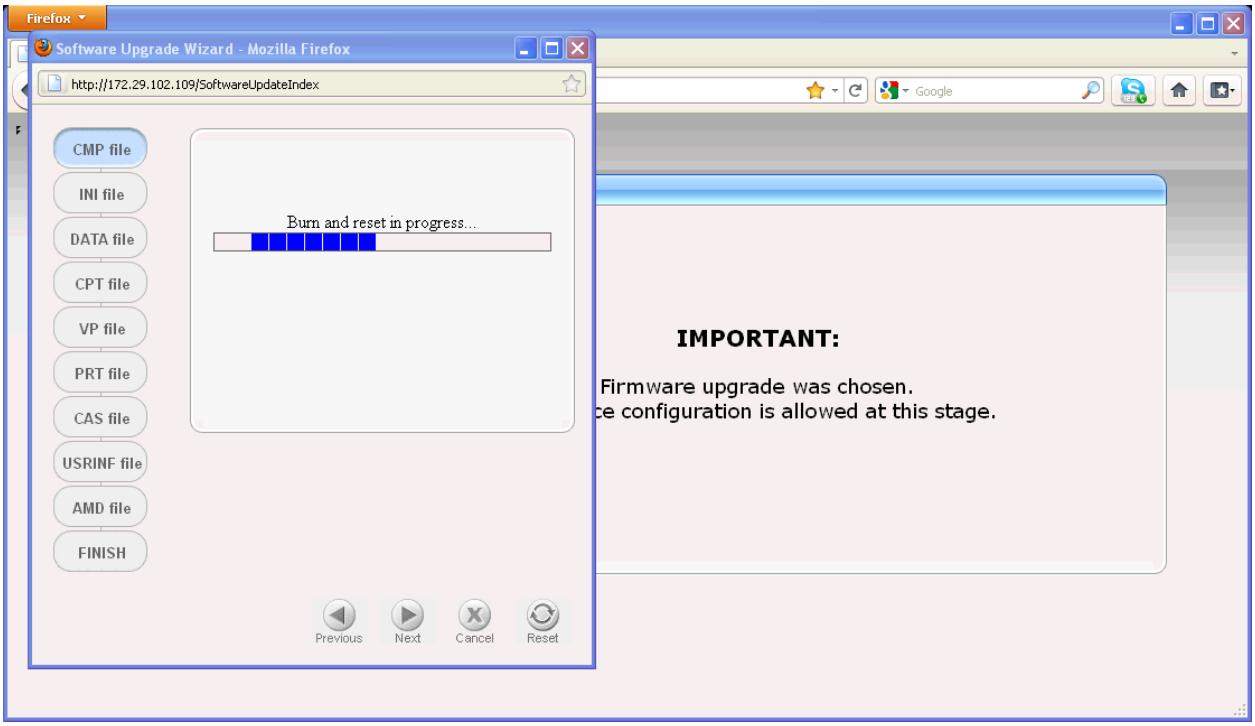

The software will load:



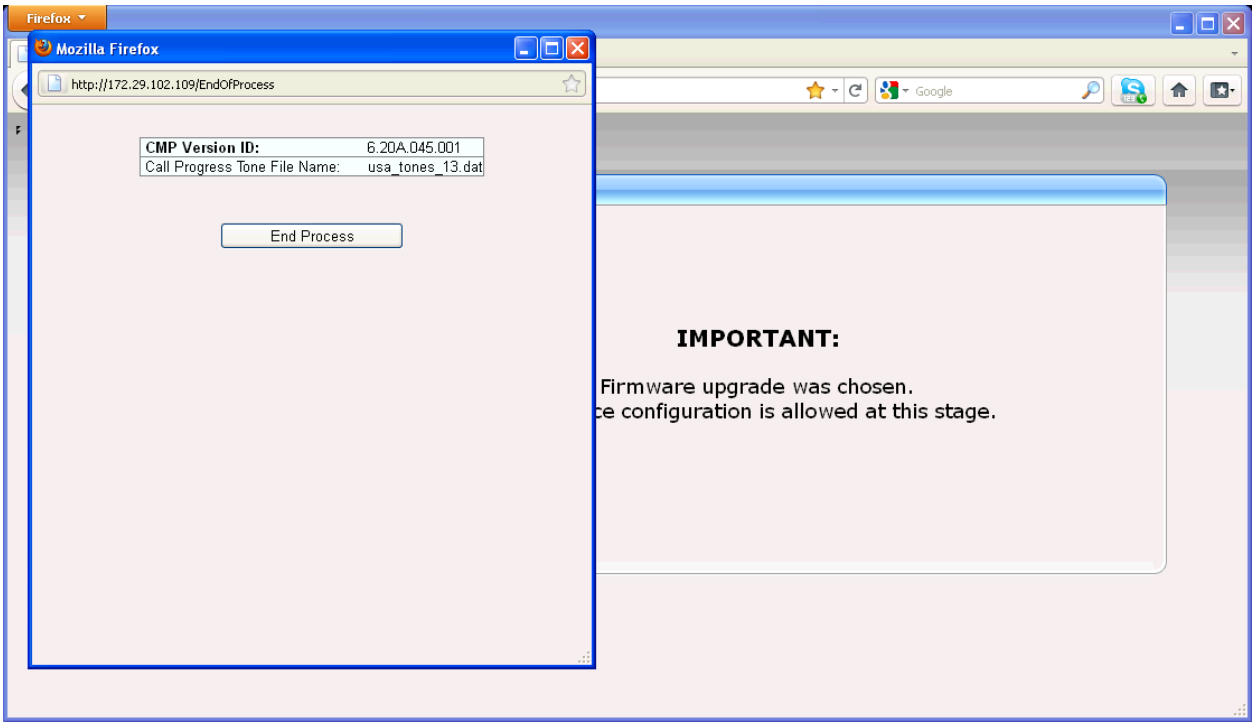

The screen will display:




Click the reset button and the Mediant Gateway will reset




After the Mediant Gateway resets, this screen displays:




Click the End Process button.

# Appendix C: Sample Files

These sample files are provided for reference and orientation. Your files will be different but will have similar elements.

## *Sample AudioCodes .ini file*

This sample board.ini file should be representative of the type of configuration you should see in a customer's board.ini file, however the configuration will vary with the number of PRI's and type of modules installed, the number ranges being used to avoid routing loops, the Mediant Gateway 's IP address and other configuration that will be site specific. This file is for reference only.

**Sample board.ini file:**

```
;Board: Mediant 1000 - MSBG
;Serial Number: 3437322
;Slot Number: 1
;Software Version: 6.20A.054
;DSP Software Version: 624AE3 => 620.10
;Board IP Address: 172.29.102.137
;Board Subnet Mask: 255.255.255.0
;Board Default Gateway: 172.29.102.1
;Ram size: 512M   Flash size: 64M
;Num of DSP Cores: 8  Num DSP Channels: 48
;Profile: NONE
;Key features:;Board Type: Mediant 1000 - MSBG ;IP Media: Conf VXML
VoicePromptAnnounc(H248.9) ExtVoicePrompt=1MB ;DSP Voice features:
IpmDetector ;Coders: G723 G729 GSM-FR G727 ILBC ;E1Trunks=4 ;T1Trunks=4
;DATA features: Routing FireWall&VPN WAN Advanced-Routing ;PSTN Protocols:
ISDN IUA=4 CAS ;Channel Type: RTP DspCh=240 IPMediaDspCh=240 ;Security:
IPSEC MediaEncryption StrongEncryption EncryptControlProtocol ;Control
Protocols: MGCP MEGACO SIP SASurvivability MSFT ;Default features:;Coders:
G711 G726;

;--------- Mediant-1000 HW components ---------
;
; Slot # : Module type : # of ports : # of DSPs
;----------------------------------------------
;      1 : FALC56      :          1 :         2
;      2 : Empty
;      3 : Empty
;      4 : Empty
;      5 : Empty
;      6 : Empty
;----------------------------------------------
```

```
[SYSTEM Params]

SyslogServerIP = 172.29.66.97
EnableSyslog = 1
NTPServerIP = 172.29.0.37
NTPServerUTCOffset = -25200
ENABLEPARAMETERSMONITORING = 1
ActivityListToLog = 'pvc', 'afl', 'dr', 'fb', 'swu', 'ard', 'naa', 'spc',
'll'
PM_VEDSPUtil = '1,79,88,15'

[BSP Params]

PCMLawSelect = 3
TDMBusClockSource = 4

[Analog Params]


[ControlProtocols Params]

AdminStateLockControl = 0

[MGCP Params]


[MEGACO Params]

EP_Num_0 = 0
EP_Num_1 = 1
EP_Num_2 = 1
EP_Num_3 = 0
EP_Num_4 = 0

[PSTN Params]

TraceLevel = 1
ProtocolType = 23
FramingMethod = D
ISDNIBehavior = 1073741824
PSTNReserved3 = 8

[SS7 Params]


[Voice Engine Params]
```

```
[WEB Params]

LogoWidth = '145'
HTTPSCipherString = 'RC4:EXP'

[SIP Params]

LOCALSIPPORT = 5080
BCHANNELNEGOTIATION = 0
CDRREPORTLEVEL = 4
GWDEBUGLEVEL = 7
ENABLEMWI = 1
IPALERTTIMEOUT = 60
TRUNKTRANSFERMODE = 2
TCPLOCALSIPPORT = 5080
TLSLOCALSIPPORT = 5081
LOCALISDNRBSOURCE = 1
SASDEFAULTGATEWAYIP = '172.29.102.137:5080'
ENABLESAS = 1
SASLOCALSIPUDPPORT = 5060
SASREGISTRATIONTIME = 60
SASLOCALSIPTCPPORT = 5060
SASLOCALSIPTLSPORT = 5061
SASBINDINGMODE = 1
SASSURVIVABILITYMODE = 1
CALLREROUTINGMODE = 1
FACILITYTRACE = 1

[SCTP Params]


[VXML Params]


[IPsec Params]


[Audio Staging Params]


[SNMP Params]


;
;  *** TABLE InterfaceTable ***
;
;
```

```
[ InterfaceTable ]
FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes,
InterfaceTable_InterfaceMode, InterfaceTable_IPAddress,
InterfaceTable_PrefixLength, InterfaceTable_Gateway, InterfaceTable_VlanID,
InterfaceTable_InterfaceName;
InterfaceTable 0 = 6, 10, 172.29.102.137, 24, 172.29.102.1, 1, Voice;

[ \InterfaceTable ]

;
;  *** TABLE DspTemplates ***
; This table contains hidden elements and will not be exposed.
; This table exists on board and will be saved during restarts
;

;
;  *** TABLE PREFIX ***
;
;

[ PREFIX ]
FORMAT PREFIX_Index = PREFIX_DestinationPrefix, PREFIX_DestAddress,
PREFIX_SourcePrefix, PREFIX_ProfileId, PREFIX_MeteringCode,
PREFIX_DestPort, PREFIX_SrcIPGroupID, PREFIX_DestHostPrefix,
PREFIX_DestIPGroupID, PREFIX_SrcHostPrefix, PREFIX_TransportType,
PREFIX_SrcTrunkGroupID, PREFIX_DestSRD;
PREFIX 0 = *, 172.29.102.137, *, 0, 255, 5060, -1, , -1, , -1, 1, -1;

[ \PREFIX ]

;
;  *** TABLE TrunkGroup ***
;
;

[ TrunkGroup ]
FORMAT TrunkGroup_Index = TrunkGroup_TrunkGroupNum,
TrunkGroup_FirstTrunkId, TrunkGroup_FirstBChannel, TrunkGroup_LastBChannel,
TrunkGroup_FirstPhoneNumber, TrunkGroup_ProfileId, TrunkGroup_LastTrunkId,
TrunkGroup_Module;
TrunkGroup 0 = 1, 0, 1, 23, 100000, 0, 0, 1;

[ \TrunkGroup ]

;
;  *** TABLE NumberMapIp2Tel ***
;
;
```

```
[ NumberMapIp2Tel ]
FORMAT NumberMapIp2Tel_Index = NumberMapIp2Tel_DestinationPrefix,
NumberMapIp2Tel_SourcePrefix, NumberMapIp2Tel_SourceAddress,
NumberMapIp2Tel_NumberType, NumberMapIp2Tel_NumberPlan,
NumberMapIp2Tel_RemoveFromLeft, NumberMapIp2Tel_RemoveFromRight,
NumberMapIp2Tel_LeaveFromRight, NumberMapIp2Tel_Prefix2Add,
NumberMapIp2Tel_Suffix2Add, NumberMapIp2Tel_IsPresentationRestricted,
NumberMapIp2Tel_SrcTrunkGroupID, NumberMapIp2Tel_SrcIPGroupID;
NumberMapIp2Tel 1 = 70xx#, *, *, 255, 255, 4, 0, 255, 3044, , 255, -1, -1;

[ \NumberMapIp2Tel ]

;
;  *** TABLE SourceNumberMapIp2Tel ***
;
;

[ SourceNumberMapIp2Tel ]
FORMAT SourceNumberMapIp2Tel_Index =
SourceNumberMapIp2Tel_DestinationPrefix,
SourceNumberMapIp2Tel_SourcePrefix, SourceNumberMapIp2Tel_SourceAddress,
SourceNumberMapIp2Tel_NumberType, SourceNumberMapIp2Tel_NumberPlan,
SourceNumberMapIp2Tel_RemoveFromLeft,
SourceNumberMapIp2Tel_RemoveFromRight,
SourceNumberMapIp2Tel_LeaveFromRight, SourceNumberMapIp2Tel_Prefix2Add,
SourceNumberMapIp2Tel_Suffix2Add,
SourceNumberMapIp2Tel_IsPresentationRestricted,
SourceNumberMapIp2Tel_SrcTrunkGroupID, SourceNumberMapIp2Tel_SrcIPGroupID;
SourceNumberMapIp2Tel 1 = 9*, *, *, 255, 255, 0, 0, 255, 303583, , 255, -1,
-1;

[ \SourceNumberMapIp2Tel ]

;
;  *** TABLE SourceNumberMapTel2Ip ***
;
;

[ SourceNumberMapTel2Ip ]
FORMAT SourceNumberMapTel2Ip_Index =
SourceNumberMapTel2Ip_DestinationPrefix,
SourceNumberMapTel2Ip_SourcePrefix, SourceNumberMapTel2Ip_SourceAddress,
SourceNumberMapTel2Ip_NumberType, SourceNumberMapTel2Ip_NumberPlan,
SourceNumberMapTel2Ip_RemoveFromLeft,
SourceNumberMapTel2Ip_RemoveFromRight,
SourceNumberMapTel2Ip_LeaveFromRight, SourceNumberMapTel2Ip_Prefix2Add,
SourceNumberMapTel2Ip_Suffix2Add,
SourceNumberMapTel2Ip_IsPresentationRestricted,
SourceNumberMapTel2Ip_SrcTrunkGroupID, SourceNumberMapTel2Ip_SrcIPGroupID;
SourceNumberMapTel2Ip 1 = *, 1xxxxx#, *, 255, 255, 6, 0, 255, unknown, ,
255, 1, -1;
```

```
[ \SourceNumberMapTel2Ip ]

;
;  *** TABLE PstnPrefix ***
;
;

[ PstnPrefix ]
FORMAT PstnPrefix_Index = PstnPrefix_DestPrefix, PstnPrefix_TrunkGroupId,
PstnPrefix_SourcePrefix, PstnPrefix_SourceAddress, PstnPrefix_ProfileId,
PstnPrefix_SrcIPGroupID, PstnPrefix_DestHostPrefix,
PstnPrefix_SrcHostPrefix, PstnPrefix_TrunkId;
PstnPrefix 0 = *, 1, *, *, 0, -1, *, *, -1;

[ \PstnPrefix ]

;
;  *** TABLE TrunkGroupSettings ***
;
;

[ TrunkGroupSettings ]
FORMAT TrunkGroupSettings_Index = TrunkGroupSettings_TrunkGroupId,
TrunkGroupSettings_ChannelSelectMode, TrunkGroupSettings_RegistrationMode,
TrunkGroupSettings_GatewayName, TrunkGroupSettings_ContactUser,
TrunkGroupSettings_ServingIPGroup, TrunkGroupSettings_MWIInterrogationType;
TrunkGroupSettings 0 = 1, 4, 255, , , -1, 255;

[ \TrunkGroupSettings ]

;
;  *** TABLE ProxySet ***
;
;

[ ProxySet ]
FORMAT ProxySet_Index = ProxySet_EnableProxyKeepAlive,
ProxySet_ProxyKeepAliveTime, ProxySet_ProxyLoadBalancingMethod,
ProxySet_IsProxyHotSwap, ProxySet_SRD, ProxySet_ClassificationInput,
ProxySet_ProxyRedundancyMode;
ProxySet 0 = 0, 60, 0, 0, 0, 0, -1;

[ \ProxySet ]

;
;  *** TABLE SASRegistrationManipulation ***
;
;

[ SASRegistrationManipulation ]
```

```
FORMAT SASRegistrationManipulation_Index =
SASRegistrationManipulation_RemoveFromRight,
SASRegistrationManipulation_LeaveFromRight;
SASRegistrationManipulation 0 = 0, 0;

[ \SASRegistrationManipulation ]

;
;  *** TABLE CodersGroup0 ***
;
;

[ CodersGroup0 ]
FORMAT CodersGroup0_Index = CodersGroup0_Name, CodersGroup0_pTime,
CodersGroup0_rate, CodersGroup0_PayloadType, CodersGroup0_Sce;
CodersGroup0 0 = g711Ulaw64k, 20, 0, -1, 0;
CodersGroup0 1 = g711Alaw64k, 20, 0, -1, 0;
CodersGroup0 2 = g729, 20, 0, -1, 0;

[ \CodersGroup0 ]
```

# Sample Phone Configuration Files

Below is a sample of the configuration files used by an 84-Series handset during the course of the testing. In this example we utilized MAC specific configuration for a phone with the MAC address of 00907a0cd96e:

**Filename: 00907a0cd96e.cfg**

```
<?xml version="1.0" standalone="yes"?>
<APPLICATION
 APP_FILE_PATH="sip.ld"
 CONFIG_FILES="sip_7001.cfg, fwd.cfg"
 MISC_FILES=""
 LOG_FILE_DIRECTORY=""
OVERRIDES_DIRECTORY=""
CONTACTS_DIRECTORY=""
LICENSE_DIRECTORY=""/>
```

**Filename: sip_7001.cfg**

```
<PHONE_CONFIG>
  <reg
reg.1.address="your extension number goes here"
reg.1.displayName="your name goes here "
reg.1.label="your extension number goes here "
reg.1.auth.userId="your extension number goes here "
reg.1.auth.password="your extension number goes here "
reg.1.server.1.address="ip address of your mediant 1000 gateway"
reg.1.server.1.port="5060"
/>
<dialplan
dialplan.removeEndOfDial="0"
dialplan.digitmap=""
/>
</PHONE_CONFIG>
```

**Filename: fwd.cfg**

```
<PHONE_CONFIG>
<divert
divert.1.contact="the number you wish the phone to forward to when you are
unavailable goes here">
<divert.dnd
divert.dnd.1.enabled="1">
</divert.dnd>
```

```
<divert.fwd
divert.fwd.1.enabled="1">
</divert.fwd>
<divert.noanswer
divert.noanswer.1.enabled="1"
divert.noanswer.1.timeout="30">
</divert.noanswer>
  </divert>
</PHONE_CONFIG>
```

# Appendix D: Information needed when you Contact Spectralink Support

To ensure that you get the best service possible, certain information about your system is required so that any service issue can be speedily resolved.

### Before logging a Service Request:

The following checklist identifies tasks that you should complete prior to logging a Service Request with Spectralink Technical Support:

- **Describe the application/network (Optional - provide network diagram)**
- **Describe when the problem started and what has recently changed. (Required)**
- **What is the software version? (Required)**
- **Have you reproduced the issue, and documented the procedure? (Required)**
- **Have you collected all the relevant logs and configuration files? (Required)**
- **Board INI file – (Required - Extract from Web interface)**
- **Syslog – (Required)**
- **Ethernet Capture – (Optional - Readable by Ethereal or Wireshark)**
- **DSP Trace – (Optional)**
- **PSTN Trace – (Optional)**